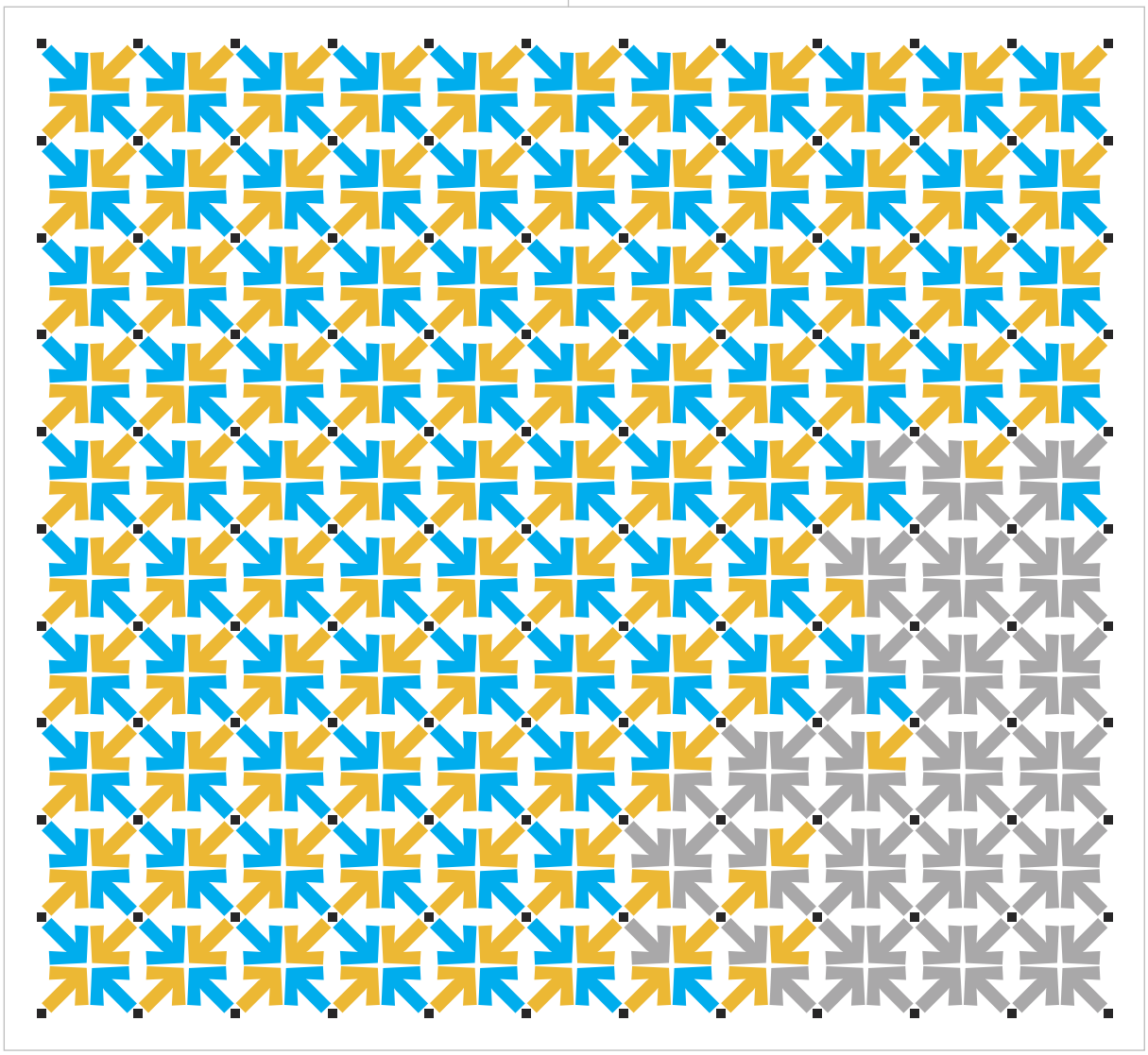


Standardizing Business Continuity

How to prepare for being prepared.

FEMA's PS-Prep: What to Expect

Private-sector preparedness is not required, but market forces may make it seem like it is.

BY LINDA TUCCI

AMERICAN BUSINESSES should soon have a better understanding of what the government expects of them in the event of man-made or natural disasters.

Two and a half years after Congress directed the Department of Homeland Security (DHS) to develop a voluntary program to promote private-sector preparedness, the federal agency is close to designating a comprehensive set of standards by which American businesses can assess their preparedness for disasters and be officially certified as having an adequate plan.

Soon, the DHS's Federal Emergency Management Agency (FEMA) is expected to officially designate three alternative business continuity standards that will be recognized by its Private Sector Preparedness Accreditation and Certification Program (PS-Prep), a joint program between DHS and the private sector designed to measure, certify and ultimately enhance business resilience.

"The genesis of this program is that Congress wanted to know if we were better prepared than we were in 2001 and better than we were in Hurricane Katrina to sustain a major catastrophe, and the answer is, 'We do not know,'" said Donald Byrne, managing director of consulting firm North River Solutions Inc., and a business continuity professional. "Part of the goal is to use this program to gauge where we are improving and where we need to invest more."

The three standards, proposed by FEMA in October and open for public feedback until mid-January, are:

- NFPA 1600, developed by the National Fire Protection Association;
- BS 25999, from the British Standards Institution; and
- ANSI/ASIS SPC 1-2209, a new standard from ASIS International.

According to DHS Secretary Janet Napolitano, the frameworks were among 25 standards considered and were chosen based on "their scalability, balance of interest and relevance to the PS-Prep program."

The DHS has also contracted with the ANSI National Accreditation Board (ANAB) to develop the accreditation rules that will allow certification bodies to go out and conduct the audits. But Byrne, who serves on the ANAB's committee of experts, said that even as PS-Prep moves forward, many issues remain up in the air, including:

- How to handle certifications for small businesses.
- How to credit businesses that have already passed more rigorous business continuity standards.
- How to determine which incentives—if any—should be offered to encourage businesses to become certified.

Indeed, questions about these issues—and recommendations—came up often in the 41 pages of letters submitted to FEMA during the public comment period. Michael Cummings, director of loss prevention services at Milwaukee-based Aurora Health Care, praised the agency's decision to approve more than one standard for PS-Prep and urged that other guidelines and best practices be sanctioned.

ONE SIZE DOESN'T FIT ALL

"This is not an area where one size fits all," Cummings said. "The ultimate goal of the PS-Prep Program should be to incentivize and assist business organizations to find solutions and approaches that work for them and not create bureaucracy and arbitrary certification programs as a barrier to accomplishing preparedness."

The question of incentives versus costs was also raised by J.D. Densmore, manager of the emergency command center at home improvement chain Lowe's Cos. Densmore said he supports standardization of business continuity across the retail industry as "an excellent goal." However, he added that he was concerned that adhering to any one standard would result in a "significant cost to any retailer," and that these costs would either erode the retailer margins or be passed on to consumers as higher cost of goods.

Businesses in general have a vested self-interest to be prepared for disaster, he said. "The business case to participate in the voluntary program needs to be compelling enough to overcome the cost, or it will not be adopted," he warned.

The preparedness program, although voluntary, should improve awareness about business continuity, an area that gets short shrift in American companies. "Most people's knowledge of preparedness amounts to the fire drill when they were in high school," said Byrne. His clients often

have little in place to deal with major emergencies, such as a violent employee or noxious fumes, "let alone keeping their business running and sustainable after a disruption."

Paul Kirvan, a business continuity expert based in New Jersey, said that giving companies a choice of three standards eligible for certification is probably better than having only one.

But deciding on a standard will require thoughtful analysis from businesses to find the right fit—and the cost can be considerable. Kirvan said that when he learned the program would be voluntary, his initial reaction was that it was doomed to fail.

COMPETITIVE ADVANTAGE

Kirvan said he doubts people will participate in a certification program unless they're required to or have a substantial business incentive to volunteer. "But I think what will happen over time is certain large businesses, Fortune 100 or Fortune 500 organizations are going to decide it is probably the right thing to do and good from a competitive standpoint," he added. "So, I think it will be competitive forces in the marketplace that will get organizations on the bandwagon for this." Kirvan also said he expects that the government program will come up with a streamlined way for getting certified.

Byrne agreed. "I am hoping the government understands that its real role in a voluntary standard like this is education," he said.

However, this step may be the first phase in setting standards that could be used to officially indemnify companies against liability for damages after a disaster, Byrne said. That aspect will likely be sorted out by the courts citing the voluntary best practices in cases, rather than written into PS-Prep.

> "What will happen over time is ... Fortune 100 or Fortune 500 organizations are going to decide it is probably the right thing to do and good from a competitive standpoint."
>
> —**PAUL KIRVAN,** secretary, Business Continuity Institute, USA Chapter

In the meantime, adopting these standards may be useful as a means for companies to assure their suppliers and customers that they are reliable in case of emergency. "In the end, there is no reason for people to do this except market pressure, and that is ultimately going to be the driving force behind this," Byrne said. ■

Linda Tucci is senior news writer for SearchCompliance.com. Write to her at ltucci@techtarget.com.

Making the Case for Business Continuity

If you decide to plan for business continuity, it's best to use a standard.

BY PAUL F. KIRVAN

THE BEST WAY to describe the current state of business continuity standards in the U.S. is "standby mode." The Federal Emergency Management Agency (FEMA), charged with implementing a Private Sector Preparedness Program (PS-Prep), as specified in Title IX of P.L. 110-53, has:

- Proposed three standards;
- Selected the ANSI-ASQ National Accreditation Board to establish accreditation and certification requirements for PS-Prep (see Chapter 1); and
- Solicited comments on its proposed standards at a series of "town meetings" in 10 U.S. cities.

At some time in the future, FEMA will release a summary of the meeting results.

QUESTIONS FOR BUSINESS LEADERS

So, what does this mean for you as a business leader? Should you look further into the standards and possibly select one for your firm to adopt? The good news is that you have three from which to choose. (There are numerous other business continuity standards; these are simply the ones the U.S. government has selected.) This is certainly better than the situation in other countries, which either have just one such standard, one that was developed in another country, or none at all.

In the U.S., business continuity traditionally has been ignored as an unnecessary expense with minimal chance of providing a return on investment—except, perhaps, in the aftermath of a disaster. In other countries, such as the U.K., Singapore and Australia, for example, business continuity is quickly becoming a key aspect of business. Standards in those countries are eagerly anticipated and readily adopted. In short, these nations "get it."

Let's return to these shores, however. If your business has anything to do with banking, investment banking, utilities and the oil, chemical, nuclear and maybe a few other vertical markets, you're aware of business continuity (or similar activities) because they're required by your regulators. The rest of U.S. businesses have no such requirement. The government appears to be gently easing us into business continuity with the PS-Prep program. At the moment, accreditation is voluntary—which kind of takes away any sense of urgency or necessity.

Let's ask some important questions: Will your business be affected—for example, shut down, penalized or fined—if you don't have a business continuity program? If your business is among the many that aren't regulated, the answer is "no."

By contrast, could competition make business continuity a desirable activity? The answer is "maybe." Here's an example: In some sectors, firms soliciting new suppliers or business partners seek evidence of business continuity programs that are documented and in use. The presence or absence of such a program may not be a show-stopper by itself, but could be the deciding factor if the finalists and their capabilities are otherwise identical. Could that affect your business?

Here's another thought: Regardless of the size of your business, you're always looking for ways to differentiate yourself from and beat the competition. Could a business continuity program provide a competitive advantage? The previous paragraph certainly suggests it.

Here's another thought: Regardless of the size of your business, you're always looking for ways to differentiate yourself from and beat the competition. Could a business continuity program provide a competitive advantage?

So, where do standards enter the game? Clearly, if you decide there are sound business reasons for introducing business continuity, will any standard do? The answer is "yes." The activities associated with business continuity are largely unchanged from their roots back in the 1960s and '70s. Sure, some processes have been updated, and lots of new definitions have been introduced. But the basic premise of business continuity—ensuring that your business can return to normal following a disruptive event—is unchanged. A closer look at the three standards that FEMA currently supports shows that—with vari-

ations in language and structure—each standard says virtually the same thing!

Can you continue business as usual without a business continuity program? Absolutely. Can your business survive without adopting a business continuity standard? Same answer. So, is it necessary to go any further? Nope. Can you go home now? Yep.

CONSIDERING GOVERNANCE

All that having been said, let's briefly examine the issue of governance, as that word describes how you run all aspects of your business. Let's assume you have invested much into your business to make it a success. Doesn't it also make good sense to ensure your business stays in business, especially when you're faced with an incident? How do you currently do that? How do you keep your business running? This is where business continuity—standards notwithstanding—becomes a key part of your firm's governance.

Assuming you decide—from the perspective of governance or competition or maybe both—that it makes sense to protect your business and keep it running, what would you do? If you decide in favor of business continuity, and it is worth the investment, use standards to help you design and establish a business continuity program. Which standard is the best for such an activity? Probably the BSI Group's BS 25999, because besides being well-organized, it is widely considered an auditable standard. Any one of the three PS-Prep standards will work, however. Do the homework and review each standard to see which most fits your organization.

If you decide in favor of business continuity, and it is worth the investment, use standards to help you design and establish a business continuity program. Which standard is the best for such an activity?

Business continuity standards are definitely right, provided you are comfortable with the rationales you use to justify business continuity. If you elect not to pursue business continuity, standards clearly make no sense. In this article, however, we have suggested a few strategies that may be worthwhile. A lot of work has gone into the current crop of business continuity standards. Each is good; each provides all you need. So, take the next step. ■

Paul F. Kirvan, FBCI, CBCP, CISSP, has more than 20 years' experience in business continuity management as a consultant, author and educator. He is secretary of the Business Continuity Institute USA Chapter.

Is There Meaningful Use for BC?

A plethora of security and risk standards throws BCM standards into question.

BY STEVEN ROSS

"THESE ARE my standards. If you don't like them, I have others."

This paraphrase of a Marxist pronouncement (Groucho, of course) seems to apply to business continuity management (BCM). It would be excellent to have a unified, consistent approach to the business continuity discipline, but what we have instead is a plethora of overlapping and somewhat contradictory statements, standards, guidelines and methodologies all purporting to be the One True Path to Enlightenment (or, at least, to recoverability).

It is therefore reasonable to ask whether, with so many standards to choose among, are business continuity management standards necessary at all? This is difficult to answer directly because behind the smoke screen of conflicting standards there are some very real questions left unanswered (or the answers are just assumed).

For example, is BCM a subset of industrial security or information security, or is it a discipline that stands on its own? Does a standard apply to a concept—the continuity

It is reasonable to ask whether, with so many standards to choose among, are business continuity management standards necessary at all? This is difficult to answer directly.

of business operations—or to a particular activity, i.e., the creation and maintenance of business continuity plans? What is the relevance of BCM to other disciplines such as the aforementioned security, but also to IT, strategic planning and risk management?

And then there is the big question,

unasked, unanswered and unanswerable: If a business continuity plan is developed in compliance with any and all standards, will it work when it is needed? As much as one would like to believe that the answer is yes, the positive cannot be proven. The fact that a plan enables an organization to recover from Disaster 1 does not necessarily mean that it will recover from Catastrophe 2. And if the answer to the big question is no, then what is the value of any standard in the first place? The fact is, no one can demonstrate that a plan that adheres to the various standards is any likelier to succeed than one that does not.

WHAT DO STANDARDS DO?

But is that the true test of a standard? We need to consider why standards are created at all. The website of the International Organization for Standardization (ISO) says that, "Standards ensure desirable characteristics of products and services such as quality, environmental friendliness, safety, reliability, efficiency and interchangeability—and at an economical cost." Do BCM standards foster these attributes (leaving aside environmental friendliness)? As argued above, they do not do so directly, but it does seem that the BCM standards, taken together, do achieve most of these goals.

The standards all, to a greater or lesser degree, say the same things: understand the organization's needs; develop a strategy that meets those needs; document the strategy in actionable plans; implement, train, test and maintain the plans. Thus, it is the processes of creation of governance, and not the resulting plans, that are the subject of the standards.

The standards all ... say the same things: understand the organization's needs; develop a strategy that meets those needs; document the strategy in actionable plans; implement, train, test and maintain the plans.

It is not that the plans are standardized and, therefore, better plans. Rather, business continuity plans developed in a standard manner are more likely to have higher quality, reliability and the rest of ISO's attributes because they take into account the successes—and the failures—of those who have developed such plans in the past.

BCM STANDARDS AND CERTIFICATION

The greatest benefit of BCM standards is that they serve as a point of reference. The fortunes of many

organizations are linked to those of their product and service providers, as well as to those of their customers. In this network of interlocked interests, the failure of one has repercussions for many. Thus, following standard practice and being certified as doing so *may* be a part of the glue that will hold an extended enterprise together. Global opinion is converging on BS 25999 as the primary BCM standard, not least because BSI offers independent certification of compliance with it.

Thus, an organization can develop a business continuity plan and a governance structure to maintain and improve over time, following or not following any standard as it pleases. Business partners wanting assurance that an organization's recovery plans are likely, not guaranteed, to work in an emergency can gain such assurance only by an audit process.

This sort of an audit may be performed directly, but there are constraints on the number of vendors that any one organization can audit, to say nothing of the vendors' reluctance to have all their customers at their doors demanding to come in and inspect the joint. Certified compliance with a standard accomplishes the audit for the company. The certifying organization acts as a stand-in for all those seeking assurance and does so by measuring the audited organization's *process*, which by implication should provide a measure of certainty about the company's recoverability.

Now, "a measure of certainty" is hardly complete assurance, but it may be the best that all involved are ever going to get. If it reduces friction among business partners, raises the level of resilience across enterprises and fosters commerce, then it is not such a bad thing. Quite a good one, in fact.

Business partners wanting assurance that an organization's recovery plans are likely, not guaranteed, to work in an emergency can gain such assurance only by an audit process.

To return to the question of the necessity of BCM standards, it seems then that the standards by themselves are not necessary and may not even be useful. But demonstrated compliance with a standard is extremely useful, and a globally recognized standard used for consistent measurement is necessary to that end. ■

Steven Ross, MBCP, CISSP, CISA, is founder and principle at Risk Masters Inc.

Measuring Continuity Risk

Uncertainty is the rule when measuring risk, so be as correct as possible.

BY STEVEN ROSS

IT IS AXIOMATIC that if something cannot be measured, it cannot be managed. It follows that risk measurement is an intrinsic component of risk management. Risk management is very much in the news these days, applied to finance, insurance and war. There are a variety of techniques used in each field, with mixed success in each and virtually no correspondence among disciplines. A common consideration of risk in business is the possibility—or rather, the uncertainty—about events that might interrupt an organization's functional and technical operations, i.e., continuity risk.

Unfortunately, the most common approaches to measuring continuity risk are vague, subjective and difficult to use for guiding management in budgeting for controls and countermeasures. Almost all are based on the simplistic formula:

Risk = Impact x Probability

There are several problems with this method of measuring risk. First, it does not measure risk at all, but rather exposure, which is the expectation of loss over time, usually expressed on a yearly basis: the ALE, or annual loss expectancy.

If members of management have a reasonable expectation of, say, $10 million in annual losses due to business disruptions, they have an outer boundary for investment to mitigate or eliminate their effects through controls or insurance. No one would spend $20 million to reduce a $10 million exposure. The proper amount is an amount (much) less than the potential impact, perhaps nothing at all (i.e., acceptance of the exposure).

As Nassim Nicholas Taleb explains in *The Black Swan*, risk is not about predictable losses but instead about the impact of highly improbable events, the so-called "unknown unknowns." Thus, *Risk = Impact x Probability* is meaningful for those disruptions for which likelihood and effects are known, or at least are predictable.

As Taleb demonstrates, it is specifically the rare, unforeseeable incidents that cause the most damage.

In other words, we will forever be uncertain about the probability of a significant disruption, a catastrophe. Other researchers such as Rory Knight and Deborah Pretty of Oxford Metrica have shown that the impact on shareholder value is magnified by management ineptitude, especially if an event results in deaths. Thus, the impact is not predictable either. The time-honored formula collapses into itself.

It is not simply time that honors the formula. The information security risk management standard ISO 27005, which includes business continuity risk, shows risk as a function of likelihood and impact.

BS 25999, the generally accepted global standard for business continuity management, explains that risk is "an average effect by summing the combined effect of each possible consequence weighted by the associated likelihood of each consequence," although, to be fair, the standard does go on to say that, "probability distributions are needed to quantify perceptions about the range of possible consequences."

It recommends instead standard deviations, which (as Taleb rants on about) lead us back to known, rather than unpredictable, effects. NFPA 1600, the U.S. standard on disaster/emergency management and business continuity programs, defines risk as —no surprise—"a combination of probability and severity."

SO WHERE DOES THAT LEAVE US?

For one thing, it leaves us without a magic formula and it seems there will never be any worthy algorithms for calculating risk. But that does not mean that risk cannot be measured. It is important for risk measurement to be accurate, but it is not necessary for it to be precise to the nth decimal place. If we cannot have a solid, quantified value for continuity risk, we can still get it right in a relative or "fuzzy" manner. Here are some basic principles:

- **Measure the effect on critical resources, not the threats to them:** Once again, poor definition leads to poor thinking. NFPA 1600 provides a list of "hazards"; ISO 27005 has its list of "threats" and "vulnerabilities." Both standards mean events like fires, floods, earthquakes, power failures or corrosion. But no one can list all the possible causes of continuity breaches. That would be betting against God, and he always wins.

The real risk to an organization is the impact on critical resources. At a high level, these resources include working premises, human resources, data, equipment, information systems, voice and data networks, raw materials, etc. The nonprobabilistic approach is to determine the effects of disruption of these resources without a *priori*

consideration of the likelihood or extent of such disruption.

- **Categorize the impacts:** The simplistic formula asks us to posit probability, without stating the specific impact we would refer to. Thus, we must assume the worst case, i.e., total destruction. That is indeed one category of impact, but so are:

  - **INACCESSIBILITY** (the resource exists, but we cannot get to it)—Consider offices on the 50th floor when the elevator does not work.
  - **UNAVAILABILITY** (the resource exists but is rendered inoperable)—Consider hacks that stop websites.
  - **UNUSABILITY** (the resource exists, but it is malfunctioning)—Consider a Voice over Internet Protocol telephone system if Internet connectivity is lost.
  - **INCAPACITY** (the resource exists and functions as expected but not at a sufficient level)—This usually occurs at a gradual pace, but consider a computer virus that slows a network to a crawl.

  Each of these categories might be adjusted somewhat to fit the circumstances of a particular resource. It is not clear how unusability, for instance, might apply to people.

- **Scale the categories:** Each of the impact categories might occur at different levels. For example, the total destruction (i.e., death) of critical personnel is one of those unpredictable events. However, the range could be expressed as the death of all critical people or the death of a single individual. Particularly for large populations, the risk of losing everyone is not credible, while the loss of just one approaches a certainty in any given time period. Even total loss may be credible if one is concerned about nuclear attack, a classically unpredictable event. The same might be said about the loss of some versus all data, raw materials or workplaces. The scale might be expressed differently for certain resources, but the concept remains the same for all.

> The real risk to an organization is the impact on critical resources.

- **Determine the credibility of each level of risk:** Note that in scaling the impact categories, the test is credibility, not likelihood. Those levels not considered credible should be eliminated, leaving only the risks that might occur to respective resources. At this point, management can begin to determine the investments it wish-

es to make to mitigate the risks. Note that the investment may be differentiated based on management's perception of relative credibility of each level, the "fuzziness" in risk measurement. Note also that some outlay is required for all credible risks, even if the risk is accepted. In that case, the piper must be paid when the tune is called.

- **Consider frequency of occurrence:** Aha! Here, probability seems to be creeping in the back door. While this is to an extent true, consideration of frequency comes in only at the end, not the beginning of the measurement. Moreover, it might be expected that some risks, while credible, would have less impact on an individual basis but might occur more often. For example, some equipment somewhere is going to malfunction on a regular basis. Recognizing this, management institutes preventive maintenance. It is the high-impact, low-frequency events (i.e., catastrophes) that seemingly absorb most of the business continuity budget, until the measurement of the totality of risk is considered.

In the end, risk measurement is a process, not a formula. Moreover, it is an unending process, because the profile of risk changes at an unpredictable pace. That is why risk management is a continuous process as well. ■

Steven Ross, MBCP, CISSP, CISA, is founder and principle at Risk Masters Inc.

SearchCompliance.com

Standardizing Business Continuity
is produced by CIO/IT Strategy Media,

Jacqueline Biscobing
Managing Editor

Linda Koury
Art Director of Digital Content

Scot Petersen
Editorial Director

Linda Tucci
Senior News Writer

Paul Kirvan
Steven Ross
Contributors

FOR SALES INQUIRIES

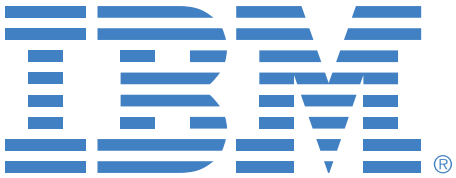
Theron Shreve
Senior Product Manager
tshreve@techtarget.com
(617) 431-9360

BUSINESS STAFF

Andrew Briney
Senior Vice President/Group Publisher

Theron Shreve
Senior Product Manager

Katie Graybeal
Marketing Manager



- **IBM Tivoli Security Operations Manager 3.1: Migrating Tivoli Security Operations Manager 3.1**

About IBM:
At IBM, we strive to lead in the creation, development and manufacture of the industry's most advanced information technologies, including computer systems, software, networking systems, storage devices and microelectronics. We translate these advanced technologies into value for our customers through our professional solutions and services businesses worldwide.
www.ibm.com