



Public sector, public trust

Epic challenges in a world of opportunities

Editor-in-Chief

Barry Gay

barry.gay@sas.com

Copy Editors

Amy Dyson

Chris Hoerter

Trey Whittenton

Editorial Contributors

Gail Bamford

Denise Bedford

Jean-Loïc Berthet

Martha Casanova

Bertrand Cayzac

Robert Charette

Linda Combs

Michael Dowding

LaVerne Durham

Mark Kagan

Kelly LeVoyer

Marie Lowman

Fiona McNeill

Trent Smith

Vincent Talucci

Art Direction and Design

Brian Lloyd

Circulation

Ellen Brandt

Production

Melody Fountain



Copyright © 2010 SAS Institute Inc., Cary, NC, USA. All rights reserved. Limited copies may be made for internal staff use only. Credit must be given to the publisher. Otherwise, no part of this publication may be reproduced without prior written permission of the publisher and copyright owner. SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. 104447_S50296.0310



Mixed Sources

Product group from well-managed
forests and other controlled sources
www.fsc.org Cert no. SCS-COC-001247
© 1996 Forest Stewardship Council



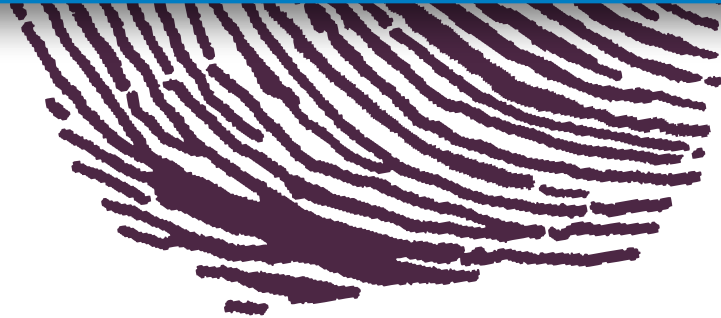
 **View Government Insights on the Web at:**
www.sas.com/gov-insights

contents

- 3 Predictive analytics:
Government's most powerful ally**
Jim Goodnight
- 4 Turbulent times call for visionary leaders**
Marie Lowman
- 6 Risk management in government**
Robert Charette
- 10 Detecting fraud with social network analysis**
- 11 Defense logistics sharpen focus on mission readiness with analytics**
Gail Bamford
- 15 Safeguarding currency value**
Jean-Loic Berthet and Bertrand Cayzac
- 19 Fighting cyberwars with cyber-analytics**
Mark Kagan
- 22 Semantic applications increase productivity in public sector**
Denise Bedford
- 25 Policing to prevent crime and disorder**
Vince Talucci
- 27 Government statistics near and far**
Marie Lowman
- 29 Making government more transparent**
LaVerne Durham
- 31 Lead—and succeed—in 10 steps**
Linda Combs
- 32 Passport Canada forecasts demand delivery with SAS®**



What if you could analyze nearly double the data you do now – and increase efficiency of fraud investigations by 10%?



You can. SAS gives you The Power to Know.®

SAS software is at work in all 15 US federal departments as well as the 50 states helping organizations make critical decisions on fraud detection and prevention, case management, financial compliance and auditing, program performance, defense logistics, cyber security and risk management.

►► www.sas.com/prevent
for a free white paper



THE
POWER
TO KNOW.®

Predictive analytics: Government's most powerful ally

By Jim Goodnight, CEO, SAS

With government customers in 80 countries, all 50 US states and all 15 US executive departments, the public sector is one of the most vital markets for SAS. Recent developments have made that more true than ever.

Government agencies have become increasingly adept at collecting data, creating both unprecedented challenges and compelling opportunities. Globalization and international crises have led to calls for collaboration and transparency across agencies, states and even countries. Traditional barriers to the effective use of data are breaking down. Now, more than ever, the time is right to apply advanced analytics that address the most important issues of our time.

That's what leads us to issue Government Insights. I hope it serves as a conversation starter for thought leaders in technology and government to share ideas, best practices and visions for how government can be transformed through sophisticated data analysis.

For instance, billions of dollars are lost every year to fraud, waste and improv-

er payments. Analytics can help ensure that the right money reaches the right recipients and help identify sophisticated fraudsters through technologies such as social network analysis.

Public security, from intelligence and national security agencies to local law enforcement and criminal justice, is a market where peace, prosperity—and lives—are literally all at stake. SAS recently made two acquisitions to help with the needs of those organizations.

The sophistication of cybercriminals is in danger of outpacing the capabilities of cyberdefenders. Predictive analytics can be a powerful weapon in protecting government networks.

Risk and financial management, taxation and auditing, infrastructure,

defense logistics and government health care are just a few additional areas that demand – and benefit from – the more effective use of analytics. Government agencies must maximize their assets to help them bear incredible responsibilities. SAS stands ready to assist them in using their most powerful asset: their data.



Jim Goodnight has been at SAS' helm since the company's incorporation in 1976, overseeing an unbroken chain of revenue growth – a feat almost of unheard of in the software industry.

Turbulent times call for visionary leaders

By Marie Lowman

The qualities that make a wise leader are not exclusive to public and private agents of power. They are precepts for anyone who aspires to lead. The qualities that make an outstanding Prime Minister are, in many ways, the same as those that describe one who gains – and deserves – peer respect as a “thought leader.”

We all strive to be thought leaders. But what does that term really mean? Is a thought leader someone who is the first to come up with a thought? It would be silly to think every idea in this publication is seeing the light of day for the first time. So how can we establish thought leadership?

Leadership is an essential quality that can only be learned, and earned, over time. Good leaders continually engage in their surroundings to learn, educate, encourage and understand – all while putting each of these characteristics into practice for the benefit of others. Madeleine Albright, former US Secretary of State under President Clinton, stated during a speech at The Premier Business Leadership Series in Berlin that leaders must have confidence, but that confidence alone is insufficient. Confidence must be accompanied by discipline and sound judgment. Otherwise, it can lead to complacency and arrogance.

As SAS’ industry marketing manager for government and health care, I’ve learned that the most critical and valuable aspect of my job is to listen. To provide the best software and services to our public-sector organizations, we must, at our foundation,



understand the challenges and issues government organizations face every day. Only through this understanding can we provide solutions that usher in a new level of citizen confidence in what our governments can achieve on their behalf.

A confident leader asks the right questions to the right people at the right time, and the answers to those questions drive everything we do. In these times of global financial and political uncertainty, it is more critical than ever to stay ahead of events in a world that never remains still. Using technology to answer the key questions – what happened and, more importantly, why – can also lead to predictive insights that not only prepare us for change, but allow us to capitalize on it.

It is my hope that, as you read through the articles in this publication, you learn

how public-sector organizations worldwide are using technology to capture and retain increased levels of citizen confidence while maintaining service levels in an unprecedented era of fiscal constraints. Technology can address specific government challenges, challenges that we learn about by listening to customers. The more turbulent our conditions, the more visionary we must be. At SAS, we want to thank you, our customers, for helping us understand the challenges you face so that we may in turn be a trusted advisor to your organization. And maybe even a thought leader at that.



Follow our blog, State and Local Connection
blogs.sas.com/statelocalgov



Marie Lowman is a Global Industry Marketing Manager with SAS responsible for the Public Sector and Health Care markets. With over 15 years of international experience, Lowman has a demonstrated understanding of the unique challenges facing these markets and works with public sector organizations around the globe to optimize their IT systems for greater transparency and accountability.

Albright's highlights:

- Confidence is an essential ingredient of leadership.
- Lead with confidence—but confidence alone is insufficient. It must be accompanied by discipline and sound judgment. Otherwise it can produce complacency and arrogance.
- A confident leader asks the right questions to the right people at the right time.
- A confident leader must have the right combination of proven principles and new ideas.
- We must stay ahead of events in a world that never remains still. Innovation is critical, but it cannot come at the expense of reliability, customer service or values.
- Confident leaders must have a healthy dose of flexibility, willingness to experiment with new approaches and the capacity to foretell the future.
- The more turbulent the times, the more visionary our responses must be.
- International coordination is essential.
- Cooperation should be a habit, not a last resort.
- There's a direct link between prosperity and stability.
- Leaders must never be driven by fear. They must be driven by hope.

Risk management in government

When the risk is measured in lives, the solution is chosen with care

By Robert Charette

A jetliner crashes. Executives at investment banks earn bonuses while investors and homeowners lose billions of dollars as subprime mortgages melt down. Tainted food poisons dozens. A new flu virus closes schools and panics parents. At first glance, it's easy to get upset at the failures in managing the public's risk and overlook the successes.

The fact is, our air travel systems, financial markets, food inspections and health care system are safe and successful virtually all of the time thanks to a government that, overall, effectively manages our nation's collective risks – risks that individuals, companies or even nongovernmental organizations like charities cannot manage alone. The US government manages public risk in numerous ways:

- For the common good. Whether it's national defense, homeland security, or emergency and disaster response, the federal government manages a broad spectrum of risks that private individuals cannot address.
- Risk regulator. The federal government regulates risks between private entities and spells out who owns risks and what levels are acceptable.

- Shaper of risk. The government also creates opportunities through structured risks. Whether it's the Small Business Administration, Defense Advanced Research Projects Agency (DARPA), or the American Recovery and Reinvestment Act (otherwise known as the 2009 stimulus program), government can create an effective environment where risk and innovation are in balance.

- Risk manager of last resort. In a variety of ways, the government provides a firewall against runaway risks to ensure stability in numerous areas, such as the financial markets. The management of this risk, of course, must be counterbalanced by not encouraging moral hazard – that is, expecting the government to always absolve one of the negative consequences of the risks taken.

- Internal risk management. Federal agencies and departments of all stripes deliver programs and services to the public. They must manage the risks inherent in their own operations to ensure citizen satisfaction and the delivery of value for money.

Introduction of ERM

At first, each risk area (strategic, operational, financial and insurable) was

ERM is rapidly gaining attention in government circles as a discipline that can significantly improve governmental performance.

managed independently, in silos. However, it soon became apparent that by adopting a holistic view of their overall risk exposures and initiatives, companies could benefit by ensuring risks were not being over- or under-managed. The concept of enterprise risk management was born. Enterprise risk management (ERM) improved the executive's ability to make better decisions that more accurately reflect the true nature of the risks in the business environment. Of course, no other organization presents both the levels of complexity and risk that the federal government faces daily. For instance, consider that, through Medicare and Social Security, the US is the largest insurer in the world. Consider also the magnitude of the strategic, operational, financial and insurable risks that the government confronts daily. Not surprisingly, ERM is rapidly gaining attention in government circles as a discipline that can significantly improve governmental performance.

Unfortunately, risk management in government isn't as straightforward as it is in the private sector. Not only is the magnitude of the consequences so much greater, there are also added dimensions in the form of politics and stakeholder

motives that extend beyond simply measuring increases in a company's profit or loss statement. On Capitol Hill alone, there are 535 "risk managers," each with differing views of the importance of risk based on local concerns and party affiliation. With every election, or news event, the priority can radically change.

Government risk managers tasked with carrying out the wishes of Congress must fashion definitions of successful risk management that reflect both pragmatism and political concerns, not merely ROI. It is challenging to quantify both the probability of a negative outcome (a failure) and the impact of that failure on citizens. As a result of scale and political dimensions, it becomes daunting to stand up and answer the questions, "What is the acceptable level of risk?" and "What losses are we willing to accept in pursuit of our objectives?" In a manufacturing context, this would be the limits of tolerance or quality control. But the federal government isn't a factory. Is it acceptable for some people to be injured by a new drug even if a vast number of others find relief from their pain and misery?

The impact of unintended consequences is much larger at this level as well.



For instance, laws to limit lead products in children's toys can go too far if they also restrict all uses of lead in motorcycle brake and clutch pedals that pose a miniscule risk to children. Decisions to destroy batches of vegetables incorrectly thought to be tainted with salmonella can cost hardworking farmers, and their insurers, hundreds of millions of dollars. However, few public officials are willing to defend decisions that may lead to even the smallest failures. And risk without responsibility is a recipe for disaster, as we've seen in instances ranging from the losses of space shuttles to Hurricane Katrina.

Manipulating risk

In recent years, this culture of preventing all failures without fully understanding the cost has become pervasive. The elemental definition of risk and risk tolerance has changed, and that's changing the fundamental assessments of risk by adding in significant uncertainty. Issues of moral hazard are far less clear today than they were even a year ago. It's impossible to simulate scenarios because political influences can disrupt the models without notice.

For instance, bondholders who have seen the bankruptcy of Chrysler and General Motors abrogate their preferred rights may fundamentally change their perception of lending risk. When longstanding rules change without any notice, and when failure can't be reasonably quantified or becomes subject to more arbitrary factors, then risk management really becomes akin to gambling. In addition, if the expectation or possibility of failure is eliminated, mark participants may have incentive to engage in risky behaviors that can diminish the government's ability to manage risk for the good of all.

Transparency is required

For ERM to be effective, risk managers, rank-and-file employees, and executives must create decision-making behaviors that value transparency. That culture can only be achieved through objective information with attainable goals. In government settings, such information makes it virtually impossible to evade responsibility and accountability. Too often, this runs counter to the prevailing culture and necessitates a transformative change that will empower people to openly discuss

On Capitol Hill alone, there are 535 “risk managers,” each with differing views of the importance of risk based on local concerns and party affiliation. With every election, or news event, the priority can radically change.

assumptions, constraints and the risks that they confront. It requires boldness, even if it means that progress is measured in small steps. But with President Obama’s directives to improve transparency and collaboration, we’re already seeing signs of improvement.

ERM, IT and government

Collectively, these three factors—government agencies’ reliance on IT and the reputational risk posed to senior executives by its failure; the Obama administration’s mandates for an open, accountable government; and White House appointments of a CIO and CTO—make government IT operational risk management an imperative. IT is also a good place to start ERM since IT risk management involves the management of strategic as well as financial risk. By initially focusing on the management of IT operational risks (the people, processes and technology needed to implement or sustain IT operations), not only can IT operational performance improve, but the beginnings of an overarching ERM framework can be laid out that goes beyond IT.

Most successful ERM programs have a top-down, senior management pull (i.e., “What are my agency’s or department’s risks?”) and a bottom-up push of objective information from the working level to answer that question. Remember, strategic decisions can’t be better than the objective information created at the program and project levels. As government’s role of risk manager expands in reaction to changing risks, and perceptions of risk, IT-led ERM will take on an increasingly greater role.



ONLINE

Find out more about managing risk in government:
www.sas.com/gov-erm



Robert Charette, President of the consulting firm ITABHI Corp., has advised federal agencies and FORTUNE 100® companies and written, lectured and consulted extensively on risk management strategies across the globe.

Detecting fraud with social network analysis

Workers' compensation fraud is a growing concern for federal and state governments. Nationally, financial crimes related to workers' compensation fraud is estimated to be in the billions of dollars annually. Approximately 10 percent of each premium paid is directly related to the cost of fraud perpetrated by employers, employees and medical providers alike.

Washington State's Department of Labor and Industries, which administers the state's mandatory workers' compensation program, has suffered its fair share of fraud in the past. In recent years, it has been tackling the issue head-on to recover as much of the estimated \$100 million it loses each year to fraud.

The Department of Labor and Industries says the types of fraud it encounters regularly can be classified under three main categories: worker, employer and health care provider fraud. Examples of basic fraud schemes include employees who work under the table while receiving compensation funds for an injury; workers who injure themselves on their own time and claim it happened while at work; and, employers that fail to report their employees for insurance, or report them as having jobs that involve less risk to pay lower premiums. Examples of medical provider fraud include billing for services not performed or for proce-

dures that were less complex than what was claimed.

"Fraud affects every worker and employer in the state – it's a tax fairness issue," says Doric Olson, Fraud Detection Manager, Washington State Department of Labor and Industries. "It drives up the rates for legitimate employers and even employees, who pay about 25 percent of the premium out of their paycheck. Additionally, in any industry in which bidding for contracts is involved, like construction, fraudulent employers can underbid by using the value of premiums they're not paying as a cushion; they're stealing work from companies that play by the rules."

Currently, the department is uncovering about \$26 million of the premium revenue lost annually and is realizing a return on investment of about eight to one. In other words, for every dollar the Washington State Department of Labor and Industries spends investigating fraud, it gets eight back.

While the department has been relatively successful in investigating and recovering a good portion of the revenue lost to fraud in recent years, the methods for doing so involved significant manual and inefficient processes. The department is now looking to build more efficiencies into its fraud detection processes, and

increase its returns by \$8 million in the short term, with the SAS Fraud Framework and SAS Social Network Analysis.

"We wanted a single solution that would help us do what we call identify resolution," says Olson. "We have to combine 20 different data sources from within our agency and other external agencies, such as the IRS, to give us a comprehensive view of a particular employer or employee. So instead of logging into multiple systems to do research, we wanted one system that would, at a glance, tell us whether we have an act of fraud or not. We also wanted a system with a good graphical interface that illustrates what is going on. This technology is very good at doing that."

With the SAS Social Network Analysis solution, the department will now be able to identify interpersonal associations and potential fraud rings, providing more opportunities to discover fraud it might not have been looking for.



ONLINE

Read more about fraud-fighting efforts in the State of Washington and in Los Angeles County at:

www.sas.com/washington

www.sas.com/lacounty

Defense logistics sharpen focus on mission readiness with analytics

By Gail Bamford

Defense logistics organizations provide essential support to the military. From enabling humanitarian relief efforts following natural disasters to sustaining troops in wartime, mission success depends on efficient and cost-effective delivery of supplies and equipment where and when they're needed.

Military supply chains are arguably some of the most complex in the world, comprised of many disparate sub-chains that collectively create a logistics ecosystem. No single organization owns them all, yet they must all work together. Managing multiple supply chains in multiple domains is a huge challenge for defense logistics organizations of all sizes, but particularly for the largest expeditionary forces, like the United States, whose supply chain is the world's largest and has more SKUs than the biggest global retailer. Decreased operational effectiveness and reduced readiness can result if the proper resources aren't at the right place at the right time.

Logistical challenges are numerous and complex. Demand patterns are unpredictable. Standard logistics processes can be slow and cumbersome. Processes are not transparent, and visibility into assets, supply chains and resources is limited. And the sheer size and complexity of the intricate

supply network that serves the logistics mission hinder effective and timely logistics support. New strategies for optimized supply chain operations are critical to balance operational readiness with cost effectiveness.

The IT perspective

Over the last decade—or longer—many defense forces have sought to modernize their logistics systems and processes. Several have even taken this to a higher level by pursuing massive defense logistics transformation programs that take years to implement and cost billions of dollars. Enterprise resource planning (ERP) models became the standard, and many European forces quickly adopted ERP systems and started focusing on modernizing their financial systems. The United States took the transformation route and made massive investments to overhaul the sprawling ecosystem supporting Army, Navy, Air Force and Marine Corps logistics.

Now that some of these programs are entering production or, in other cases, maturing, many countries are realizing that ERP is not the be-all, end-all solution they anticipated. One expected outcome of an ERP implementation is the ability to make better decisions. But are these newer systems en-



abling better decisions? Are decision makers, planners, supply officers and commanders able to do their jobs more efficiently and better complete their missions? The results are mixed at best.

Data, data everywhere

You can't make good decisions without good data.

Whether data is created and stored in newer ERP systems, locked in legacy systems, or maintained in desktop files such as spreadsheets, logistics and complementary support systems are awash in data. Some of it is useful – but some is little more than a waste of disk space. What's more, there is a lot of potentially useful data being collected, but nobody knows how to make sense out of it.

“Understanding how the data is going to be used becomes a critical factor in applying technology,” says former Institute for Defense and Business Executive Fellow Lt. Gen. Claude V. “Chris” Christianson, USA (Ret.), who was the director for logistics, J-4, until he retired in 2008. “Just collecting the data by itself isn't good enough. It needs to support

a decision-making process and enable people to make better decisions.”

Accessing the right data – and only the right data – to make the right decisions can be one of the biggest challenges. Currently, logistics data is stored in all kinds of formats, but is often incomplete or of bad quality. Some data is structured and neatly stored in relational databases or other organized formats. Other data, such as unstructured data from log books, is harder to incorporate into decision making.

In the end, good decisions in logistics affect readiness and operational effectiveness. Until recently, readiness was a measurement that seemed to be mutually exclusive from cost. However, as defense forces have continued to cut costs, readiness at any cost is no longer acceptable.

“If I have and can use the data to improve the reliability of a system, then I will not have to buy so many spare parts, and the cost comes down,” says Vice Adm. Walter B. Massenburg, USN (Ret.), a current Executive Fellow at the IDB, whose last assignment was Commander of Naval Air Systems Command in Patuxent, MD.

“If I have and can use the data to improve the reliability of a system, then I will not have to buy so many spare parts, and the cost comes down.”

Vice Adm. Walter B. Massenburg, USN (Ret.)

Decision-making challenges

ERP systems have consolidated many proprietary legacy systems that once operated in silos. However, even today, gaining access to good, complete data is still a challenge because so much data still exists in disparate locations, formats and quality. Good decisions still depend on good and complete data. Forward-looking defense logistics organizations are moving past reactive historical reporting and adopting proactive stances for planning and operations. They use the data they have more effectively to make supply chains and logistics operations more efficient. Given today's economic climate, most governments want new ways to become more efficient and reduce costs without getting involved in high-cost, high-risk IT projects. Data integration and business analytics solutions that complement current systems can yield affordable results and quickly demonstrate significant ROI. Here are some examples of how SAS is helping military organizations address logistics challenges:

Management of materiel in transit

Gaining visibility into materiel in transit is a very big challenge in expeditionary forces. Not knowing the status of materi-

el or when it can be realistically expected can cause all kinds of unintended consequences – mostly related to the lack of confidence in the system. Bad habits have developed over time, and hoarding of supplies/spare parts used to be common place. One retired government official once said that good supply officers order three of everything – one for stock, one in case the other one doesn't arrive, and one to trade. A very expensive way to do business!

The Ministry of Defence (MoD) in the UK wanted to improve management, planning, and tracking of essential supplies and equipment from the UK to its operations deployed around the world. The goal was to provide front-line commands with the ability to plan procedures with greater certainty.

“Together with HPES (EDS), SAS is helping provide the MoD logistics community with detailed information on how each step in the supply chain is performing and helping to identify areas for improvement – at a level of detail not previously possible,” says Roy Martin, a SAS employee and former Information Systems Strategy officer in the UK MoD's Defense Logistics

Organisation. “Reduced duplication provides a clear cost and efficiency benefit. There is also a clear military effects benefit arising from the increased confidence in delivery for front-line commanders who can use that to plan for a higher tempo of operations.”

Maintenance forecasting and planning

Maintenance expenditures consume a large part of defense budgets. Current conflicts are drawing limited resources from proper maintenance and recapitalization of battle-wearied equipment. Too often, maintenance is either reactive after a costly failure or routine – whether it's needed or not.

“Forecasting for maintenance capabilities is a complex, multi-disciplined, cross-organizational task,” says John Wenke, retired Department of Defense executive and president of Blue Heron Services, a small logistics engineering consulting firm. “This is especially true in environments where multi-mission military equipment is used in different theaters of operation with significantly different environments and operational requirements. A great deal of valuable information about equipment is collected over its life cycle by operational, mainte-



Babbitt talks supply chain

General George T. Babbitt, USAF (Ret.) is a member of the class of 2009-2010. In 2000, he retired from his role as Commander of the Air Force Materiel Command at Wright-Patterson Air Force Base.

Here are some of his thoughts on improving the military supply chain:

“In the end, our logistics systems still need to be adaptable and respond to an uncertain future. I’ve said to many people that I didn’t think there would ever be a time when we would be able to forecast the future reliably. But, on the other hand, I don’t want to discount the importance of careful data collection. By collecting recent historical data and analyzing it effectively, we can certainly narrow our forecast for future outcomes.

“In my mind, a supply chain is adaptive when it can respond to the future even when events that unfold are not the way we had planned them. Military commanders plan for the future, but they also expect the unexpected. Logisticians should be no different, but often we are. Military logistics has been based for generations on average demand. When the real world unfolds and demand doesn’t turn out the way we expected, we’re dismayed as if it had never happened before and we immediately go into a mode of trying to better estimate the average demand for the future. . . . What we need to do is better understand the variability of the future and build more adaptive systems.”

Listen to General Babbitt’s Point of View video, “Change Management, The Key to Successful Logistics Management,” at

www.sas.com/gov-babbitt

nance and supply organizations. But the full value of the data is often not realized to the extent possible.”

SAS helps maintenance planners exploit the full value of their data and achieve their goals of enhancing the material condition and maximizing the flightline availability of aircraft. Using data mining and advanced analytics, maintenance planners can now explore data in unique ways to expose new insights. This results in higher systems availability, lower support costs, and more efficient maintenance forecasting and planning.

Total asset visibility

Along with the drawdown of troops in Iraq goes the responsibility for properly resetting and disposing of equipment. Ultimately, equipment will either be redistributed within theater, retained with prepositioned stocks, transferred to other locations engaged in military operations, donated to foreign governments, or disposed of. Remaining equipment gets returned to the home country for repair and refurbishing.

Gaining visibility into equipment stores that include 60,000 to 80,000 containers, 50,000 vehicles and approximately 3 million different pieces of equipment is an enormous effort. SAS helps a military logistics organization support the

reset of this equipment by helping commanders see equipment locations and conditions so they can decide what to do with it. Should they return it to its home base or send it to the repair depot? Should they deploy it into another geographic area, leave it behind, or destroy it? In past drawdowns, losing track of equipment – permanently – was not uncommon. This effort goes a long way toward improving the military’s stewardship of taxpayer funds.



SAS is a sponsor of the Executive Fellows Program at the Institute for Defense and Business. www.idb.org/about/idb-executive-fellows

Gail Bamford is an Industry Marketing Manager with SAS and has over 25 years experience helping IT companies develop marketing and sales strategies to address complex problems in the public sector, including defense logistics and national security. She is actively involved in collaborative efforts to respond to the cybersecurity challenges that confront government agencies.

Safeguarding currency value

It takes comprehensive economic intelligence – especially in tough times

By Jean-Loïc Berthet and Bertrand Cayzac

Emperor

I've heard enough of these endless how and when. / We're short of money. Good: get money then.

Mephistopheles

I will. A surplus too, you have my word. / Easy enough, but easy things are hard.

It's there already. The whole art / Is getting at it. Who knows where to start?

Johann Wolfgang von Goethe
Faust, Part II

Goethe knew what money is to nations. As a privy counselor to the Grand Duke of Saxe-Weimar, he engaged in state duties as hyperinflation raged in America and then in France, in the wake of their revolutions. No wonder that, in *Faust*, the devil himself creates paper currency to expand the country's money supply. This makes him an authentic central banker, though a radically ill-considered one.

Whatever inspires man's monetary ingenuity, modern central banks are concerned with controlling its powerful innovations. If their missions have anything to do with the battle of good against evil, the latter certainly goes by the name of monetary instability.

Indeed, price volatility blurs the signals required to make rational economic decisions, hinders efficient resource allocation and distorts competition. While monetary stability does not prevent financial crises, inflation shocks have directly resulted from many (such as the Argentine peso and Thai baht collapses in the 1990s). Although conventional wisdom holds that financial stability depends on monetary stability, that view is increasingly facing skepticism. Most

central banks target price stability as a primary, if not sole, goal. Despite this consensus, international central-bank coordination is a difficult political issue, especially when it comes to exchange rates, as illustrated by current tensions over dollar-yuan parity.

So, easy things are hard. Indeed, to formulate monetary policy and steer its instruments with reasonable accuracy in a changing global environment, central banks must weave a comprehensive economic intelligence capacity into their decisions.

Large bureaucratic structures must collect and process vast amounts of heterogeneous economic, financial and monetary data, then distill elaborate information, aggregated indicators, model-based projections and analyses that are the basis of risk assessments of price stability. Eventually, the governing body applies informed judgments to make its decisions.

All along this process, harmonized auditable data infuses communication, especially among stakeholders such as supervisors and regulators, peer central banks, international institutions or states.

The *de facto* standard

As a standard in the academic world, SAS® analytical solutions have been widely adopted by economists and economic analysts across central banks worldwide. They are a *de facto* standard for sharing data and models as part of cooperative schemes.

Today, SAS integrated platforms are not only deployed to bring the online power of advanced data management and analytical functions to the analyst's desktop; they are deployed as part of a wider vision to empower the economic R&D with end-to-end control over information processes.

With increased autonomy in accessing, processing and disseminating data, the business lines can develop and refine their complex programs much faster to match the challenging environment.

This agility is often sought as a strategic objective and backed by the IT department, where SAS operability and transparency are instrumental in tailoring highly reliable, cost-effective open architectures to solve business problems and align with overall strategy.

www.sas.com/ba

Economic and monetary statistics are essential because accountability to citizens is paramount.

Economic intelligence

Following standards from the International Monetary Fund and the Bank for International Settlements, central banks, regulators and nations have developed statistical frameworks together with analytical functions to guide their policies and disseminate information. While the relationships among these bodies vary within and across countries, they often achieve strong levels of cooperation, at least regarding economic and financial statistics production. At the international level, they maintain strong ties with supranational entities and with the academic community as information providers, contributors to theoretical frameworks, and employers.

The data sources, their cascades and their modes of processing are numerous and heterogeneous. Rather than attempt to describe them all, we provide this example from the European Central Bank (ECB) to shed light on the typical elements and their articulation:

With the ECB's federal structure, regular policy preparation is essentially fed by data from 16 member-nation central banks and their statistical ecosystems.

This data is structured along two main threads: economic and the monetary analysis.

The economic indicators are output and its components, demand and labor market conditions, price and cost indicators, fiscal policies, asset prices and financial yields, sentiment indicators, and balance of payments. Note that, as a comprehensive statement that systematically summarizes economic transactions with the rest of the world, the latter is itself a critical, highly complex framework involving many aggregates as part of the compilation of national accounts.

The monetary indicators are monetary aggregates and their counterparts (ranging from notes and coins to saving deposits and money market funds in several standardized combinations), credit aggregates (assets of banks' balance sheets), loans to the private sector, money-based inflation-risk indicators, measures of excess liquidity, indicators of the monetary policy stance, and interest rates.

These two sets of indicators are jointly processed in model-based macroeconomic projections, quarterly monetary assessments, time series, factor and dynamic stochastic equilibrium models.



The resulting high-level analysis comes along the two threads again: an assessment of short-to-medium-term determinants of inflation on the economic analysis and an analysis of monetary trends on the other side. They are cross-checked and form the overall assessment of risks to price stability upon which the Governing Council makes its decisions.

The regulatory bodies are not formally accounted for in the above scheme. However, the risk information they control plays an increasing role in central-bank decisions, especially when the systemic stability of the banking system is endangered. Recent crisis management has demonstrated that a strong organizational integration of central banking and regulatory functions brings the most acute analysis.

It would take a separate article to describe the vast amounts of data at stake, the quality and integrity issues, and the many layers of aggregation and computation involved.

As a whole, this endeavor to monitor economic activity represents a significant effort that can be viewed in terms of employees, budgets, data volumes, publications and more. But it might be more relevant to evaluate its worth relative to the value created or even to the

value-destruction avoided or mitigated.

This is the realm of decision making and action.

The central banker's helm

It is with an eye on these parameters that policymakers take action. Conventional monetary policy instruments consist chiefly of open-market operations with the main refinancing operations playing a pivotal role in steering interest rates, managing liquidity and signaling policy stances. The two other instruments are the standing facilities that provide and absorb overnight liquidity and the minimum reserves requirements that credit institutions must meet to stabilize interest rates and adjust liquidity.

With recent short-term interest rates at or near zero, these instruments have been complemented everywhere by unconventional measures targeting the cost and availability of external finance to banks, households and nonfinancial companies. Whether it's a direct acquisition of financial assets (direct quantitative/credit easing) or loans with longer maturities against a wider range of eligible collateral (indirect quantitative/credit easing), these policies significantly affect the central bank balance sheet while amounting to a massive risk transfer to the lender of last resort, especially when

it comes to highly illiquid assets, such as sovereign bonds whose markets are impaired (for example, Greek debt and the ECB's Securities Markets Programme).

While the infrastructures that control conventional instruments still require improvements such as indicators and models harmonization, with large discrepancies among established integrated economic zones and emerging countries, unconventional measures require vast increases in analytic power.

For example, pricing the financial assets held by central banks has always been challenging. However, properly designed risk models that analyze illiquid complex products are a high priority today. (Consider that the 2008 sub-prime crisis was not foreseen by legacy risk models.) It will be even more urgent upon recovery when the special measures are unrolled and excess assets are exchanged. Given the hundreds of billions of dollars at stake, the infinite variety of papers, the speed and unpredictability of markets, and the shifting regulatory landscape, there is much work ahead for central banks.

More generally, the forces that shape central bankers' tools in the future include improved integration of the new sources of systemic and financial instability in the models, added data from private financial entities, and stronger institutional linkages as part of a more harmonized regulatory framework. Keeping up with globalization will increasingly require high-frequency or near-real-time information.

The known challenges are enough to focus energies on quickly improving the instruments. Some of the threats to monetary stability – aside from systemic financial risk – include the serious economic imbalances between the US and Asia, the risk that inflationary strategies come to the fore again, the hidden costs of very low interest rates, and the deflationary scenarios at the heart of collective predictive analysis. Addressing these will help the world weather further instability.

More than ever, smart and comprehensive open-analytical systems will be essential to support the changes and the innovations that will emerge from these troubled times.

Jean-Loïc Berthet is a SAS Implementation Consultant. He is based in France.



Bertrand Cayzac is the SAS Account Manager for Banque de France. He actively contributes to the development of global sales to central banks and regulatory bodies.

Fighting cyberwars with cyber-analytics

Mark Kagan

All government agencies – worldwide – must accept the fact that they are engaged in cyberwarfare.

Were the United States at cyberwar, it would lose.

That's what Mike McConnell, former US Director of National Intelligence, told the US Senate in February.

Many government officials would probably assert that the US is already engaged in cyberwar, although it has not reached the point where attackers are taking down critical infrastructure (85 percent of which is privately owned), disrupting communications, or shutting down agencies. Many government officials from other countries might also say that their countries are engaged in cyberwars, though perhaps on a smaller scale – *perhaps*.

The trend is clear. For example, the number of incidents reported by US federal government agencies to the United States Computer Emergency Readiness Team (US-CERT) soared from 5,503 in 2006 to 16,843 in 2008 – a 206 percent increase. The number of incidents was almost surely understated because the report covered only *detected* incidents. In the always-on, always-connected world today, a new computer, if unprotected, can be scanned within seconds and infected with malware within minutes.

An army of millions

The types of threats and attacks are many and growing in volume, sophistication and agility. They come from foreign nations, criminal groups, hackers, hacktivists, disgruntled insiders and terrorists. The most serious, sophisticated and persistent attacks come from foreign governments and organized crime groups – sometimes working in tandem – that directly or indirectly employ hundreds of thousands of well-trained, highly motivated hackers and engineers.

The United States is by no means alone in bleeding terabytes of sensitive, proprietary, classified information and intellectual property. It just happens to be the biggest target.

The threats and attacks include denial of service, distributed denial of service, exploitation, logic bombs, sniffers, Trojan horses, viruses, worms, spyware, war-dialing, war-driving, spamming, phishing, spoofing, pharming and botnets – often in various combinations. PandaLabs estimates that 99.6 percent of all e-mail traffic directed to government mailboxes comprises spam or malicious messages – only 0.4 percent is legitimate.



Cyberwars, by the numbers

206: Percentage increase in *detected* incidents against US federal agencies (2006-2008)

8: Number of months that malicious software typically runs on government computers before detection

99.6: Percentage of all e-mail hitting government inboxes that is either spam or malicious

0.4: Percentage that is actually legitimate

Concern greater than ever

Cyberdefenders are most concerned with attacks, particularly from insiders, aimed at stealing, modifying or destroying data. The relatively recent phenomenon of advanced persistent-threat attacks has raised the level of concern even higher. These attacks penetrate organizations and insert software programs that repeatedly steal or modify data – and typically exist for as long as eight months before being detected.

Government IT managers are losing sleep because the data they must protect is growing by terabytes every month. They are inundated by masses of disconnected, uncorrelated data from all of their security systems. At the same time, the disparate and diverse systems that typically constitute IT infrastructures make it practically impossible to gain a comprehensive view of cybersituational awareness.

More sophisticated threats

Overworked and overstressed cyberdefenders spend most of their time plugging holes, fighting fires and patching their networks. They operate in perpetual catch-up mode against increasingly

sophisticated attackers who rapidly respond to security fixes with newer, more sophisticated threats.

Some government agencies have established cybersecurity operations centers, which are great for network monitoring. But they haven't provided operators and analysts with the tools to understand what drives the attacks, intrusions and anomalies – what it all means, and what's going on. While dashboards and security information and event-management systems are great for reporting what's happening and what happened, they're not much use in detecting and analyzing patterns, predicting future attacks, issuing alerts and warnings, or sketching out what-if scenarios.

According to Zalmay Azmi, the former CIO of the US FBI, in today's cyber environment, *all* government agencies worldwide must increasingly accept the fact that they are engaged in cyberwarfare. In such an environment, says Azmi, cyberanalysts will need to employ tools and processes that correlate data, improve situational awareness and alleviate shortages of qualified IT security personnel.

Forget script kiddies and hackers in basements – more often than not, the attackers are foreign governments and/or transnational criminal organizations.

Weapon of choice: cyber-analytics

Analytics can provide many of those tools and processes through statistical analysis and modeling – much as analytics can be applied to fraud detection, financial management or human resources.

Cyber-analytics can provide governments with enhanced and complementary capabilities and situational awareness about the security of their systems, networks and enterprises. It does this by monitoring activities; uncovering vulnerabilities, threats and patterns; integrating disparate data to find patterns and trends; and predicting future threats and attacks so agencies can take proactive measures to protect their data and networks.

Cyber-analytics can help government agencies meet two of their biggest challenges: coordinating cybersecurity efforts and producing practical metrics to quantify the effectiveness of those security efforts.

Cyber-analytics can also:

- Provide near-real-time monitoring that automatically generates attack alerts while simultaneously dramatically reducing the number of false positives.
- Aggregate, correlate and merge data from all network monitoring devices and other sources to provide

enhanced network domain and situational awareness.

- Detect and score the severity of possible attacks before they happen to support prevention and timely interventions.
- Provide early recognition of anomalies in network traffic and uncover otherwise hidden relationships and behavior patterns that might indicate low and slow attacks.

Analytics contribute to a holistic view of the entire chessboard – where the pieces are located, both white and black. This holistic view helps government organizations significantly improve the coordination of their cybersecurity efforts and produce metrics that provide a more accurate picture of those efforts. Finally, analytics enable governments and corporations to better understand, use and protect their data, regardless of volume, condition, state or location.

Mitigating security risks

Government cyberdefenders can no longer follow the outdated paradigm of protecting the perimeter and patching,

plugging and putting out fires. They can no longer view cyberspace tactically and react to threats and attacks, instead of taking a strategic view and being proactive. The threats and attacks are growing too fast and sophisticated and the enemies are smart, resourceful and agile. Forget script kiddies and hackers in basements – more often than not, the attackers are foreign governments and/or transnational criminal organizations.

Using analytics for cybersecurity enables government agencies to think and act strategically, be proactive in mitigating security risks, and defend their data and IT infrastructure. With analytics, IT security managers can become strategists who always look three or four moves ahead and play offense as well as defense. In other words, they can stop playing checkers and start playing chess.



Download the white paper, Cyber-Analytics for Network Situational Awareness:
www.sas.com/gov-cyber

Mark Kagan is a Washington, DC-based consultant and writer and long time analyst on defense and foreign affairs, security, and intelligence. He began his professional career as a defense intelligence analyst.

Semantic applications increase productivity in public sector

By Denise Bedford

In the past decade, we've seen semantic applications emerge from the laboratory and into enterprise settings. Forward-looking knowledge organizations are learning that semantic technologies can support a wide range of business processes. Semantic technologies go beyond a simple data retrieval by applying rigorous natural language processing (NLP) methods to model human decision-making processes, and – perhaps most importantly – they can integrate existing organizational knowledge.

Semantic technologies, in this context, involves the processing of recorded knowledge in a meaningful way – a way that represents how people think about things. These technologies use several different methods, including concept extraction, rule-based classification, dynamic classification, guided summarization and cross-language translation.

Productivity improvements

Semantic analysis can improve the productivity of analytical decision making and information and knowledge processing, and increase the effectiveness of knowledge discovery. Organizations use semantic technologies to increase productivity by processing higher volumes of information than previously

possible. Semantic technologies can reduce the time to process an institutional document from 30-40 minutes to less than two minutes. At the same time, the quality of processing significantly improves, because we are explicitly codifying the mental processing steps. As a result, the opportunity costs of using subject matter expertise for standard information management tasks can be significantly reduced without risking access to organizational knowledge.

Organizations increase productivity when they design and configure these technologies in sustainable enterprise applications, rather than as one-off projects. Semantic technologies are no longer the new IT toys. Nor are they “silver bullets” for tough knowledge challenges. They are most effective when they're deployed to do what people do, but faster, more consistently, and/or with less effort. This frees an organization's intellectual capital to do even more.

Where can an organization achieve the greatest productivity gains through semantic technologies? For many, it's in information and knowledge processing of unstructured data or text. For example, organizations have used:



- Rule-based concept extraction methods to capture key numerical indicators such as project numbers, contract numbers, unique IDs, digital object identifiers, ISBN (international standard book numbers) and other key financial numbers, with high levels of reliability and quality and minimal or no human effort.
- Grammatical concept-extraction methods to characterize market reports, or new stories with high-precision sentiment analysis.
- Grammatical concept extraction to construct descriptive maps of knowledge domains and dynamic clustering methods to illustrate the relationships of concepts within a domain.
- Rule-based categorization methods to retrospectively organize large collections of critical business documents to support faceted search with minimal human investment, or to automatically and reliably classify current content to country focus.

Achieving productivity improvements

Successful implementations result from deep modeling of business processes and integration of organizational knowledge sources, using well-planned

project development life cycles and patient learning and fine-tuning of results.

Deep modeling of business processes

Sustainable use of semantic technologies means integrating them into everyday business processes. This means modeling and exploring existing business processes for appropriate “semantic opportunities.” It means having an idea of the type of productivity gains you’re seeking before you begin. Business architects have important roles to play in implementing semantic technologies. This is not just the role of engineers or programmers.

Considered technology selections

Too often, technology decisions are based on a shallow understanding of how the technologies work and what they are designed to do. Managers often fall into the “I have a hammer, so everything looks like a nail” syndrome. It isn’t necessary to understand the statistical or parsing methods at a research level in order to decide whether a semantic technology has the functional components to support a business process.

Sustainable semantic technologies are not out-of-the-box products. Rather, they are founded in well-designed architectures, including exposable and configu-

Semantic technologies
reduce the time to
process an institutional
document from
30-40 minutes
to less than
two minutes.

rable knowledge bases, open matching rules, definable algorithms and interoperable semantic products. Semantic solutions have functional components – just like other applications. It is critical to ensure the semantic functions are fully supported by the technology you choose. Not all so-called semantic technologies are designed for enterprise use.

Neither are all “semantic technologies” able to process unstructured information in meaningful ways. Many technologies bundle NLP analysis so tightly with statistical processing that they are impossible to implement because they are “canned” applications. As a result, some are suited to only a small set of structured data processing problems. They may not be able to process unstructured data except as statistically occurring data bits.

Organizational knowledge

A 21st century semantic technology can consume existing organizational knowledge. However, a smart technology will not require this knowledge to be encoded as deeply embedded rules. Organizational knowledge is always evolving. Smart technologies consume but don’t control organizational knowledge sources. Just as we no longer embed data into program code (we learned that lesson back in the 1990s), we should never embed organizational knowledge into semantic technology.

Semantic technologies must be able to use different kinds of knowledge – represented as different kinds of structures. One size does not fit all types of knowledge. In fact, knowledge design and representation is a critical success (or

failure) factor in implementing semantic technologies. Knowledge architects and knowledge engineers play critical roles in effective implementations.

Some semantic technologies require intense programming, making it difficult for either subject matter experts or knowledge professionals to work with and fine-tune them. Subject matter experts should be the primary users of any design model for a semantic solution.

Smart lessons, smart technologies

Knowledge organizations in the 21st century will find semantic analysis technologies to be a core, strategic application. They will be extensible, flexible systems configured for their purpose and designed to scale up or down. Semantic analysis technology is not a “silver bullet” solution to all business challenges. In fact, most successful implementations of semantic technologies will be seamlessly and invisibly integrated into business processes.

Successful experiences result from a deeper understanding of the semantic elements of your business processes, taking the time to investigate the products, a willingness to invest in new and different knowledge roles, and a willingness to commit to ongoing support and expansion. When organizations make firm commitments and investments, they can realize substantial productivity gains.



“Beyond Search-and-Retrieval”: Download the white paper on enterprise text mining
www.sas.com/gov-text

Denise Bedford is a Goodyear Professor of Knowledge Management at Kent State University, specializing in the economics of information and intellectual capital methods and management. Formerly, she served as Senior Information Officer at the World Bank in Washington, D.C. and has worked at NASA, Intel Corp. and Stanford University.

Policing to prevent crime and disorder

By Vince Talucci

The conceptual framework for the modern-day professional police force can be traced back to a 19th century British cabinet-level official named Sir Robert Peel. In the Metropolitan Police Act of 1829, Peel focused upon key tenets – legitimacy, community integration and use of force. However, the crux of the policing mission is found in the first of the abovementioned tenets: “The basic mission for which the police exist is to prevent crime and disorder.”

Peel’s philosophies provide a baseline for policing today, a baseline that serves as a compass for SAS’ approach to advancing today’s police force. Prevention is as sound an idea today as it was in 1829. Fortunately, law enforcement tools available to support the concept today are a bit more advanced.

Reality bites: The challenges

Many police agencies today struggle by running from call to call. The reactive “calls for service” model focuses on short-term responses, drains finite resources and prohibits longer-range strategic approaches to solving community problems.

Many law enforcement challenges are the product of sea changes that have occurred within the last decade – most notably since the terrorist attacks of Sept. 11, 2001. The changes include:

- The need to integrate data internally and share information externally. The linking of previously disparate data repositories serves as a core function of the nation’s fusion center system.
- Law enforcement agencies grappling mightily with what to do with the data they derive from new and improved technologies.
- Staff cuts – both sworn and civilian – brought on by the global recession, while stakeholder and community demands have increased.

These changes have created significant cultural and operational challenges for law enforcement – data influx, increased information stovepipes, reduced staffing and heightened community safety expectations.

Strategic opportunities abound

With challenges come opportunities. But how can we help police agencies move from theory to action? The potential future directions can be illustrated by the following questions:

- How can law enforcement change the existing business model?
- How do we move from the reactive “calls for service” model to a preventive policing approach?
- How do we best use the information that we already collect?



- What information do we need from others? How can we get it?
- How do we optimize our available resources?
- How do we prevent the next crime? The questions no longer focus solely on changing a business model for change's sake – the questions now, and the resultant opportunities, are driven by necessity.

Law enforcement agencies will not likely see an influx of funds or staffing anytime soon. Thus, leaders must think strategically about how to best prevent crime and disorder while managing fiscal realities. Further, data from today's policing technologies piles up in disparate databases to support disparate activities. For today's police leaders, these challenges are real, and it's essential for them to optimize their available resources – staffing and data.

SAS and preventive policing

SAS understands Peel's theoretical underpinnings and the practical challenges facing our nation's law enforcement agencies today. We also understand how to optimize available resources and support law enforcement's prevention mission. How? We can accomplish both by:

- Integrating massive amounts of information in multiple disparate systems. SAS provides data-driven insights to help guide decision making.
- Applying advanced analytics to prevent crime by detecting and anticipating criminal activities, traffic crashes and other threats to civic life.
- Providing needed information in a meaningful format to decision makers – from police executives to line officers – and guiding resource allocation as well as prevention, intervention and/or suppression tactics.

SAS can help law enforcement agencies and practitioners establish a robust, information-led framework that supports innovative efforts to reduce crime, disorder, victimization, vehicle crashes and other threats to community and officer safety.

Rooted in the foundation

SAS' market-leading analytic capacity provides meaningful tools to support law enforcement's strategic and tactical approaches – and to anticipate, and consequently forestall, criminal activity. Sir Robert Peel's prevention focus still resounds today. SAS embraces this history, the challenges it poses, and the opportunity to help law enforcement agencies.



Read more:

www.sas.com/gov-police



Vincent Talucci is a Senior Industry Consultant with SAS' State and Local Government practice, serving as primary liaison to the police community. A former director of the State and Provincial Police Division of the International Association of Chiefs of Police, he served on the executive leadership team, represented the policy interests of US state police organizations and maintained oversight of IACP's information-sharing, homeland-security and technology efforts.

Government statistics near and far

Statistics offices benefit developed and developing countries

By Marie Lowman

More than 70 different countries use SAS in their statistics offices.

Four of the most impoverished countries in the world are now using SAS solutions to make fact-based decisions to help their struggling populations. Thanks to the unique partnership between SAS and Statistics Norway, the statistics offices in Moldova, Eritrea, Malawi and Uganda are building and supporting statistical capacity, enabling the governments to support the fundamental needs of their populations.

Statistics Norway is the central Norwegian office for governmental statistics. Through its international development division, Statistics Norway has cooperated with sister organizations in developing countries for more than a decade and contributed to the development of their statistical systems and capacity building. This contribution involves the strengthening of individual skills as well as developing the national statistical office as an institution.

High-quality statistics contribute to economic growth, poverty reduction, good governance, democracy building and international comparability.

The partnership program through SAS and Statistics Norway offers low-income or low-middle-income countries SAS Analytics Pro software. Statistics

Norway provides staff members that travel to the recipient country and remain on-site to provide the necessary installation and knowledge transfer to use SAS. Using SAS, the statistics offices can identify their populations' needs and disseminate the information to the necessary government, public, private and nonbusiness organizations.

Statistics offices around the world

The United Nations Statistics Division lists profiles for each country statistical office around the globe. Country profiles include a history of the country's statistical system, its legal basis, details on the statistical program and much more. You can browse country statistical office profiles at the UN site: www.sas.com/unstats

Tellingly, more than 70 different countries use SAS in their statistics offices for programs that range from census analysis and government reporting to financial planning and resource planning. Continue reading to learn about some of them.

The Australian Bureau of Statistics

uses SAS to ensure the integrity of data and statistical outputs across many divisions. John Preston, an Assistant Director in the Methodology Division



says, “Many of our collections have thousands of units – a unit being an individual or business – and with such a high number of records, SAS makes our tasks more efficient, especially as many of the procedures we require are already pre-programmed into SAS.”

Statistisches Bundesamt, the German Federal Statistics Office, replaced older, non-portable mainframe programs with SAS products, including customized applications. “The SAS solutions covered both our basic types of work – short-term ad hoc analyses as well as periodic evaluation processes – better than all other products available on the market.”

Statistics Denmark uses SAS to collect and analyze census data without knocking on doors or asking any questions. Instead of a traditional

household-based census, Denmark’s tallies are completely register-based. “We run SAS on all of our systems, and it plays a vital role in our processes,” says Lars Thygesen, Director for User Services at Statistics Denmark.

The US Census Bureau uses SAS to create person-level and household-level files for each US state and to merge records so analysts can look at components of a household. Next, analysts merge that data with geographical information so they can analyze by geographical hierarchy.



UN statistical office profiles:
www.sas.com/unstats



Marie Lowman is a Global Industry Marketing Manager with SAS responsible for the Public Sector and Health Care markets. With over 15 years of international experience, Lowman has a demonstrated understanding of the unique challenges facing these markets and works with Public Sector organizations around the globe to optimize their IT systems to ensure greater transparency and accountability.

Making government more transparent

By LaVerne Durham

The relationship between government and citizen is in a fragile state. A 2010 Pew Research Center survey reports that just 22 percent believe they can trust the federal government almost always or most of the time – one of the lowest measures in half a century. Increasingly, the public is demanding greater visibility into government decisions, actions and results – particularly those involving their tax dollars. They are also calling for higher levels of accountability. The public wants to have confidence that the government is making and implementing sound decisions.

The need for transparency

In his first full day in office, President Barack Obama embraced the importance of transparency by issuing a memo ordering the development of an open-government directive to make government open and accountable. The president declared that:

- Government should be transparent. Transparency promotes accountability and provides information for citizens about what their government is doing.
- Government should be participatory. Public engagement enhances the government's effectiveness and improves the quality of its decisions.
- Government should be collabora-

tive. Collaboration actively engages Americans in the work of their government.

By taking this action, President Obama expressed his belief that the government could begin to win back the public trust, strengthen democracy and promote efficiency and effectiveness in government.

What does transparency mean?

Transparency means demonstrating that decisions are fact-based and use complete, relevant data. However, obtaining the accurate and timely data needed is often perceived as insurmountable or costly because it is typically spread across multiple agencies or departments. Many government managers feel that making a decision that's partially based on facts is the best that can be done. Getting all the right data may have been difficult or costly in the past, but it is becoming less of an issue – or excuse – today.

Making knowledge powerful

Good, fact-based decisions can't be made without good data to start with. Technology plays a pivotal role as the government moves toward becoming more open and transparent. Data cleansing and preparation techniques combined with advanced

analytical technologies—such as data and text mining—are allowing government agencies to analyze and share insights more efficiently and accurately than ever before.

“There are solutions available today that allow government agencies to lower the cost of capturing and producing information needed to make quality, fact-based decisions,” says John Stultz, an analytical consultant at SAS.

“These tools can bring data from many disparate systems and in many different information formats into an environment where you can extract it, cleanse it, transform it and load it so that it becomes ‘analytically ready’ for decision making.”

Creating this capability can help to reduce public mistrust that sometimes occurs when different government agencies put out conflicting information.

“By having a capability to capture data from many different sources and then trust the content used for analysis,” Stultz says, “the government can present ‘one version of the truth’ to the various stakeholders interested in obtaining relevant information.”



Open to the public

The US government continues to take important steps to become more open, transparent and accountable by providing data and information to the public. Here are three recent examples:

- **Recovery.gov** – This site gives taxpayers easy access to user-friendly tools to track spending data related to the American Recovery and Reinvestment Act (ARRA) of 2009 and allows for reporting of potential fraud, waste and abuse.
- **Data.gov** – As a priority open-government initiative for the Obama administration, this site increases the ability of the public to find, download and use data sets generated and held by the federal government.
- **Usaspending.gov** – As required by the Federal Funding Accountability and Transparency Act (FFATA) of 2006, this site provides access to government spending data.

The value of transparency

The US Coast Guard Acquisition Directorate is a firm believer in openness and transparency, says Greg Cohen, Chief of Business Management and Metrics. The Coast Guard manages a multibillion-dollar investment portfolio that includes multiple programs and 22 major acquisition projects. SAS® is helping the agency bring all of its accounting data together to give its managers as well as its congressional overseers insights they never had before.

“We have three accounting systems,” says Cohen. “We can now look at five or six years of data in real time. We never had that capability before.”

Possessing that insight allows the Coast Guard to better manage acquisition resources. For example, Cohen explains, “It used to be that if an executive wanted to know what the financial status of a project was, they would put in a data call, everyone would run around, and two weeks later you would get an answer back, and it probably was wrong.”

“Now those reports are e-mailed to hundreds of people on a weekly basis. So everyone knows the status and we can manage the money and project much more efficiently,” relates Cohen.

This is critical in times of tight budgets where Congress and the president’s administration are looking to cut programs. When congressional requests come in on program or project status, the Coast Guard can confidently answer them with fact-based, up-to-date information.

Being able to see accounting information in real time also makes the Coast Guard programs more accountable, says Cohen, which is a good thing from a taxpayer perspective.

Cohen emphasizes that being able to ask the right questions, and having the right information, are keys to being open and transparent. Plus, that information is also critical for showing stakeholders – Congress, the public and the media – what and why something is being done by the Coast Guard.

Renewing public trust

The public mistrusts government because all too often they don’t have insights into how decisions are being made, or who is responsible for making them – so they naturally believe the worst. In this new age of transparency and accountability, governments need access to the right information to make sound decisions.

Moving forward, embracing a fact-based decision approach – utilizing technologies available today – will greatly help in creating a more open government and renewing public trust.

Editor’s note: Robert Charette, President of consulting firm ITABHI Corp., contributed to this article.



Read more on government transparency:
www.sas.com/gov-transparency

LaVerne Durham is an Industry Marketing Manager with SAS. She is responsible for developing marketing and sales strategies to address complex problems facing government agencies.

Lead – and succeed – in 10 steps

By Linda Combs

Do you want to be a leader in your organization, department or agency? Do you want to make daily contributions that really matter? Do you want to be known for efficiency, effectiveness, smart decisions and excellent results?

If you haven't yet met these standards, what will it take to set you apart? The answer is better information – that is, making the commitment to using analytics for fact-based decisions.

So ... where to begin?

1. **Decide what is causing your organization the most pain.** What processes are not working? What decisions are you often forced to make – when you wish you had better supporting analysis? What information do you or others – upstream or downstream – need, ask for, or want that you currently can't access? Do you already have the information somewhere in an undistinguished mountain of data? Are you data-rich and information-poor? Can the format be improved? What tools do you need? If you have a finance or budget component, are you doing all you can to contain operational costs and root out inefficiencies?
2. **Choose only a few things to change. Focus on clear, simple wins.** Do you need better ways to track fraud, defaults, improper payments or regulatory compliance? Do you need access to information or more accurate information delivered faster, without having to ask? Do you need a better dash-

board to stay on track? Do you need more automated alerts, color-coded data, or more specific data profiles?

3. **Communicate. Collaborate. Clarify. Celebrate!** Does your organization have information that another group would find useful? Are you missing information that could be easily obtained if you collaborated with another department or agency? Do you constantly try to clarify data and analyses with “what if” questions and scenarios? Are you frequently engaging others by asking, “What do we learn from this analysis or this additional piece of information?” Do you celebrate with your organization when it predicts an outcome based on analysis done by one of your employees or with new business analytics software?
4. **Honor the processes you set up.** Good processes that work smoothly bring added efficiencies and effectiveness. Expect employees to follow policies and processes. This discipline will give employees time and opportunity to move from merely managing raw data to creating and measuring meaningful metrics and then on to analysis, forecasting and predicting.
5. **Align with enterprise objectives.** How do the metrics you review fit into the department's overall operations? Do they

serve the overall mission? Do they help control costs? Do they help manage risk in your area and minimize risk across the entire department or agency?

6. **Get the right tools and technology you need.** Do you need to institute a competency center for analytics? A help desk for analytics? Or a repository of best practices and newly discovered analytical tools that you can share across your division or the entire department?
7. **Be a good role model.** Are you setting the right leadership example by making the best possible fact-based decisions and helping colleagues become better, fact-based decision makers? Are you constantly challenging yourself and your peers to measure what matters?
8. **Focus on the future.** Do not look only at historical data. Instead, use historical information to formulate predictions and improve decisions about the future.
9. **Believe things can be better.** People can work smarter; processes can improve; tools and technology can be embraced. You and your organization can make better decisions if you have better analytics.
10. **Believe you can make a difference.** There are leaders at every level, in every division, in every department and agency. You can be one of them.

Linda Combs is the former controller, US Office of Management and Budget, Washington, D.C.

Passport Canada forecasts demand delivery with SAS®

Only a decade ago just 25 percent of Canadians owned a passport. Today that number has more than doubled to 57 percent. And while Passport Canada is a government organization, it doesn't receive any funding, which means it has to generate enough revenue to cover its expenses – from employees to real estate – without making a profit. With constant fluctuations in demand for passports, it turned to SAS to help forecast future demand.

For Passport Canada, forecasting is essential to determining revenues and resources needed in the coming fiscal year. Demand over the past couple of years has been inconsistent, however, partly due to new US regulations that require Canadian citizens to be in possession of a passport to cross the border into the United States. As a government agency, Passport Canada makes efficient service delivery to the Canadian public a priority; by employing analytics, it ensures the quality and timeliness of its passport application process.

“Buying a passport is not something you do every day,” says Hubert Laferrière, Director of Strategic Management with

Passport Canada, who is responsible for economic analysis and business planning. “You don't plan to buy a passport. You plan to go on a trip, and then if you need a passport you'll buy it.”

And that means demand is inconsistent. Similar to a retail business, Passport Canada is selling a product – which in this case consists of new passports and renewals of previous passports – and it needs to manage the revenue of that product for its operations.

When the first phase of the American passport requirement occurred in 2007, Passport Canada predicted a 7 to 8 percent increase in demand and ended up with a 20 percent increase. This disconnect served as a catalyst for change when it came to forecasting patterns of demand. The analytics team, which consists of five to six analysts depending on the season, was spending most of its time capturing and cleaning data, rather than using that data to develop models and forecasts or developing a true business intelligence capability.

The analytics team chose to work with SAS Forecast Server, which generates large quantities of high-quality forecasts



quickly and automatically, allowing organizations to plan more effectively for the future. Using this solution, the team has been able to come up with highly accurate forecasts – within 0.01 percent – and understand the context of fluctuations. To date, analysts have reduced time spent capturing and cleaning data by 10 percent.

These forecasts help determine the operating budget, which affects all other functions of the organization – from HR to IT.

“Using SAS Forecast Server, we’ve started to understand behaviours of applicants,” says Laferrière.

Passport Canada has learned, for example, that people in Ontario have a tendency to buy a passport three to four months in advance, while people in Quebec and the Maritimes buy at the last minute.

“The behavior in terms of acquiring a passport is different across the country, and this information helps us align our resources with these patterns” Laferrière says. “And at a regional level, we can use different parameters to adjust demand.”

When there’s a slowdown or increase in demand, the agency can adjust to shifts through the use of part-time and casual employees. This data can also be used to model new initiatives, determine if a new delivery channel is necessary, make adjustments to a current channel or make improvements to products.

The analytics team provides forecasts three times a year for the upcoming 12 to 18 months, but also provides monthly reports at the national, regional and office level. These reports provide specific indicators in areas such as production, capacity, human resources and costs versus revenues, and are sent to all directors of the organization so key decision makers receive information regularly.

But there are also benefits for its most important stakeholder: the Canadian public. Analytics is being used to improve services, such as determining the shortest wait times in specific passport offices across the country. And Passport Canada is able to turn around a five-year passport in less than 10 business days, which ranks as one of the fastest, still secure, systems in the world.

Passport Canada is on an ongoing quest for more data to provide more indicators for forecasting. The agency is working with SAS on a data integration solution that will automate its data preparation through SAS Data Integration Studio and model business processes through SAS Activity-Based Management. In addition, SAS has provided consulting services and on-site training for analysts.

“We don’t have a lot of resources, so we have to be careful how we spend money, and that’s why it’s important for us to have these tools and develop a discipline to use that information,” says Laferrière. “For us it’s about producing sound forecasts and having the right information, at the right time, to make decisions. Ultimately it’s about improving the service we provide to Canadians.”



ONLINE

Read the full story at:

www.sas.com/success/passport-canada.html

SAS[®] for Cyber Security

Real-Time Monitoring of Networks | Historical Trending and Analysis
Aggregation of Massive Data Volumes | Detection of Future Threats

**What if you could more accurately detect the 10%
of security threats that require immediate attention?**

You can. SAS gives you The Power to Know.[®]

SAS for cyber security combats threats using cyber analytics for complete and real-time situational awareness of your entire network through monitoring, integrating, uncovering and predicting.



▶▶ www.sas.com/cybersecurity
for a free white paper