



THE VISIBLE OPS HANDBOOK

STARTING ITIL
IN 4 PRACTICAL STEPS



Information Technology Process Institute

KEVIN BEHR, GENE KIM AND GEORGE SPAFFORD

THE VISIBLE OPS HANDBOOK

**STARTING ITIL
IN 4 PRACTICAL STEPS**

Information Technology Process Institute

KEVIN BEHR, GENE KIM AND GEORGE SPAFFORD

"Visible Ops", "ICOPL" and "IMCA" are trademarks of ITPI. ITIL is a registered trademark of the UK Office of Government Commerce and not the ITPI. Capability Maturity Model, CMM, CERT, and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. All other trademarks and company names are the property of their respective owners.

For more information, please contact:

ITPI
2896 Crescent Avenue
Eugene, Oregon 97408
Main Telephone: (541) 485-4051
Main Fax: (541) 485-8163
<http://www.itpi.org>
info@itpi.org
ISBN 0-9755686-0-4

Credits

Copy Editors: Crystal Behr and Ron Neumann
Graphics and Production Manager: Harold Metzger
Project Coordinator: Mary Matthews
Technical Editor: Tom Good
Book Design: Integrity Design and Marketing

Acknowledgements

The ITPI offers a special thank you to a number of important contributors. Without the knowledge, hard work, and dedication of the following individuals, we would be challenged to produce the important tools which help to shape IT for our time.

Scott Alldridge	Charles Hornat	Mike Prospect
Julia Allen	Joe Judge	Jackie Shaffer
Ruby Christina Bauske	Rich Llewellyn	Bill Shinn
Brandon Casey	Dwayne Melançon	Troy Thompson
Grant Castner	Craig Morgan	Jan Vromant
Steve Darby	Bill Murray	Dan Waite
Jeremy Epstein	Stephen Northcutt	Henry Wojcik
Ruby Gates	Nevin Oliphant	Ron Zika
William Hertling	Fred Palmer	

Testimonials:

"A frequent complaint of ITIL consultants is that not many ITIL implementation tools are publicly available. For the experienced IT Service Management practitioner, it sometimes seems we have to re-invent the wheel each time. Visible Ops fills a big part of that void. It provides a practical insight in how to kick-start an IT Service Management improvement effort. Its common sense approach and very readable style give this book a mandatory place in the library of any IT manager. Visible Ops is indeed comparable to the manual for an Emergency Room of a hospital. I particularly liked the fact it does not pretend to be an operational 'bible' for the phases beyond the ER.

Visible Ops describes four steps to control an IT environment. The unassailable logic behind these steps is based on the practical experience of the authors, Gene Kim and Kevin Behr. These same steps can easily be mapped to any maturity model and Visible Ops hence describes a roadmap to maturity.

The first two phases of Visible Ops help organizations control the infrastructure. The third Visible Ops phase helps organizations control the services, in the spirit of Service-Oriented Architectures and IT Service Management. The last phase of Visible Ops helps organizations control the strategic value, which provides an opportunity for IT to align itself with the business and to gradually maximize its 'bang for the buck.' The easy mapping between the Visible Ops phases and any maturity model validates the compelling logic of the book."—JAN VROMANT, ITSM CONSULTANT

"Gene and Kevin have hit the preverbal 'IT nail' right on the head. When I educate customers on the benefits of documented and repeatable procedures such as ITIL and COBIT, they are always concerned about the complexity and where to start. Visible Ops creates a logical starting point and details the key 'issues and indicators.' This handbook is a 'must read' for IT Managers and Directors who are implementing a mandate from their CIO or Board of Directors to become compliant for auditors and federal regulations."—HENRY E. WOJCIK, DIRECTOR, ENTERPRISE SERVICE MANAGEMENT, NETWORK DATA SYSTEMS, INC

"The Visible Ops Handbook is the Rosetta Stone that the IT industry and its leadership have been seeking to allow them to communicate the value of ITIL to the business. Visible Ops is simple and clear, provides a roadmap of how to make an IT department not only perform better, but also to deliver more value back to the business. Without doubt, each of the four steps they outlined have value and are well supported."—DANIEL S. WAITE, SENIOR CONSULTANT, BMC SOFTWARE

"The Visible Ops handbook provides a great roadmap for IT executives to see their way through the thicket of chaotic operations and into the clearing of repeatable processes. It follows in the footsteps of software development processes like the Capability Maturity Model (CMM), and offers the potential to provide a real ROI by reducing the effort in wasted firefighting."—JEREMY EPSTEIN, SENIOR DIRECTOR, PRODUCT SECURITY, WEBMETHODS, INC.

"Finally, a 'best practice' that is based upon research and industry knowledge. Too often, best practice papers are written with little or no influence or research from those actually performing the work in the real world. This approach is a step-by-step, methodical approach for any organization looking to get a grip on Change Management and improve operations. The books format and introduction of methodologies will set the pace for all future publications!"—CHARLES HORNAT, GLOBAL INFORMATION SECURITY MANAGER

“Visible Ops provides the IT practitioner at any level with a catalytic approach to improving operational controls. The Visible Ops toolset helps organizations find a toehold in spite of sheer cliffs of chaos. If you are looking to start or improve configuration management, champion a repeatable server provisioning process, and institute meaningful metrics that breed quality decisions, Visible Ops is the place to start. I recommend this to any IS Management, as well as any senior management with a technical background or IT staffers with management ambitions.”—BILL SHINN, SECURITY ENGINEER

“If you are in IT, you are most likely currently dealing with issues of firefighting due to rampant changes, or are deliberately ignoring them due to lack of time and resources. Visible Ops provides a clear-cut methodology and steps to effectively deal with these issues. This book provides a scaleable template that fits around any size shop to get back in control, and then actually stay there. They show you how to regain control of critical changes, whether it's an entire data center rebuild, a single device failure, or upgrading an entire server farm to a new software release, and then continue to manage them effectively from deployment to production to retirement.”—TROY THOMPSON, ITIL CERTIFIED CONSULTANT

“This is a very valuable resource for anyone just getting started. If this resource had been available when I was putting together the Change Management plan for our department, it would have saved me many hours of research. I highly recommend it as both a reference and developmental tool. It will help you identify the processes and order in which you should develop and implement the various ITIL BS 15000 process areas. More importantly the tips for audit preparation will help you identify the specific areas of improvement and help you identify and target areas requiring an organizational culture change. Well written, easy to follow, with good examples; It has everything you need from beginning development through the measuring the results.”—JACKIE SHAFFER, SYSTEMS PROJECT ADMINISTRATOR, FLORIDA DEPARTMENT OF EDUCATION

“In general, this book provides a synopsis of the techniques and methodologies we at SIAC use to provide close to ‘five nine’ uptime for our owners and customers.”—MIKE PROSPECT, VICE PRESIDENT, SECURITIES INDUSTRY AUTOMATION CORPORATION

“Visible Ops is a methodology that comprehensively responds to major issues I have raised over and over again in my long career in financial and technology auditing. To attest to the reliability of systems, auditors need to see: controls in place, controls documented, controls communicated, and evidence of the controls in action. Visible Ops shows IT managers how to build their operational processes so they can answer the auditors’ eternal question: ‘How do we really know?’”—RUBY CHRISTINA BAUSKE, LEAD TECHNOLOGY AUDITOR, CPA, CIA, CISA, CISSP

“Change management done wrong is painful, cumbersome and results in needless firefighting. However, effective change management done correctly enables IT operations and information security to work more efficiently and better support the business objectives. Furthermore, it makes audits easier to pass and perform. The Visible Ops book clearly explains in a practical and manageable approach what it takes for organizations to implement change management that really works. If organizations agree to follow the approach in this book and stick to it, they will see how structured and disciplined change management will actually make their lives easier, will not stifle responsiveness or flexibility, and will help to extinguish many of the fires.”—CRAIG MORGAN, CISSP, PRINCIPAL SECURITY CONSULTANT, ENSPHERICS (A DIVISION OF CIBER)

“As an IT consultant, I continually deal with many people from different disciplines who are smarter than me. Even so, they often ask me which books I rely on to do my job. The Visible Ops book just became one of them—in my toolkit, I’d always want a pocket knife, a can of Sterno, a compass and this guide.”—RON ZIKA, ITSM CONSULTANT

Foreword

I remember well my first substantive conversation with Gene Kim in March 2003. We were in Orlando, Florida, sitting at the bar after a full day of mind-numbing security conference presentations. During this exchange, I found out what Gene was up to, and I had one of those proverbial light bulb moments. What if we could find a way to define mature IT operational processes and then embed well-defined security controls within these processes? If we could do this, we could make great progress in addressing security in the normal course of operational business, instead of by individual heroics. What made this promising and exciting was that Gene had seen this in action, and had studied how certain organizations that he called “best in class” were not only doing it, but doing it exceptionally well.

Gene introduced me to his partner in crime, Kevin Behr. We found that we had similar interests, and embarked on finding a useful way to work together. By July of 2003, we had a collaboration agreement in place between Carnegie Mellon University’s Software Engineering Institute and the IT Process Institute. In October 2003, we co-hosted the first Best in Class Security and Operations Roundtable at the SEI, bringing together leaders and high performers in IT operations and security.

On this journey, I have learned the following from Gene and Kevin:

1. They have a unique ability to observe, analyze, and synthesize information and experiences from organizations operating across a wide range of market sectors. In doing this repeatedly, they have created value, resulting in strong, long-term relationships of trust with their clients and partners.
2. They have identified critical characteristics of what it means to be high performing in IT operations and security, as evidenced by an organization’s culture, beliefs, behaviors, capabilities, and actions. They have observed how high performing organizations view the problems as well as the solutions. This handbook codifies much of this work.
3. They passionately believe in, and have begun to demonstrate, the power of mature process definitions to bring about stability and control in complex IT environments, including the requirement for auditable and verifiable controls.
4. They have invested significant time and energy in their own education (and mine) and in building a rich value network of leading and respected professionals in IT operations, security, and audit to assist and advise this work.
5. Their observations and experiences (and those of their clients and partners) on the current state of IT operations and security are remarkably similar to those of the software development community before the existence of a body of community-accepted software development process definitions (as captured in the SEI’s Capability Maturity Model® for Software).

Why has the SEI embarked on this journey with ITPI? We share a mutual desire to improve the condition of IT operations and security. These capabilities do not stand alone; they live in an enterprise context. The tougher aspects of improvement are in people and process, even though the community at large still tends to view localized technology solutions as the path for improvement. We share the belief that sustained improvement requires the creation of an executive-level community of practice, who will integrate the goals and objectives of IT operations, security, audit, risk management, process management, project management, and governance. All of these capabilities are required to bring about an operational environment that can deliver repeatable, predictable, defined, secure, measurable, and measured operational processes, thereby achieving operational excellence.

We share the objective of helping organizations make common sense common practice. By addressing the difficult questions, “How and where do you start?” this handbook is a significant step in the right direction.

Julia Allen
Senior Member of the Technical Staff
Carnegie Mellon University, Software Engineering Institute
Networked Systems Survivability Program, home of the CERT® Coordination Center

Table Of Contents	
Copyright	2
Acknowledgements	2
Testimonials	3
Foreword	5
Introduction	8
Something Must Need Improvement—Otherwise, Why Read This?	8
What You Do And Do Not Need To Know	9
Structure Of The Book	9
Visible Ops	10
History Of Visible Ops	10
Common Characteristics Of High-Performing IT Organizations	11
Why Did We Use ITIL?	12
Why Visible Ops Works	14
Visible Ops—Key Characteristics	16
Facilitating A Productive Working Relationship Between IT Operations, Security And Audit	16
An Overview Of The Four Visible Ops Phases	17
Visible Ops In Detail	18
Phase One: “Stabilize The Patient” And “Modify First Response”	19
Issues And Indicators	19
Stabilize The Patient	21
Electrify The Fence	22
Modify First Response: The Catalytic Key	23
Create The Change Team	24
Create A Change Request Tracking System	25
Start Weekly Change Management Meetings (To Authorize Change) And Daily Change Briefings (To Announce Changes)	25
Miscellaneous Change Management Do’s And Don’ts	28
The Spectrum Of Change	29
What You Have Built And What You Will Likely Hear	29
Phase Two: “Catch & Release” And “Find Fragile Artifacts” Projects	32
Issues And Indicators	32
Implement A “Catch & Release” Project	33
Find Fragile Artifacts	34
Prevent Further Configuration Mutation	34
What You Have Built And What You Will Likely Hear	35

Phase Three: Create A Repeatable Build Library	38
Issues And Indicators	38
Create A Release Management Team	39
Create A Repeatable Build Process	41
Create And Maintain The Definitive Software Library (DSL)	42
Create An Acceptance Process Contract	43
Moving From Production Acceptance To Deployment	44
Define Production Plan For Patching And Release Refresh	44
Close The Loop Between Production And Pre-Production	45
What You Have Built And What You Will Likely Hear	46
Phase Four: Continual Improvement	48
Metrics And How To Use Them	48
Other Improvement Points	50
A Caution About Automation	52
What You Have Built And What You Will Likely Hear	52
Summary	53
Information Technology Process Institute (ITPI)	54
Appendix A: Preparing For Audit	55
Controls 101	55
Auditors—Internal And External	57
The Sarbanes-Oxley Act Of 2002	57
Increasing Your “Auditability”	58
Auditor Red Flags And Indicators	60
Appendix B: The Information Technology Infrastructure Library (ITIL)	61
Appendix C: Focusing Efforts With An Integrity Management Capability Assessment (IMCA)	65
Appendix D: A Glossary Of Terms	66
Appendix E: CMDB Table Structures	68
Appendix F: Reference List	70
Appendix G: High-Performing IT Organizations: What You Need to Change to Become One	72
About The Authors	78
Kevin Behr	78
Gene Kim	78
George Spafford	78

Introduction

Practitioners in information technology (IT) face pressures on many fronts. In addition to the demands to become more efficient, IT must now address challenges to maintain a secure state and comply with regulatory requirements. For example, the Sarbanes-Oxley Act of 2002 is forcing publicly held U.S. corporations to attest to the fact that internal controls are both in place and effective. IT operational best practices, such as the Information Technology Infrastructure Library (ITIL), provide a framework to start defining repeatable and verifiable IT processes. However, as organizations attempt to use ITIL to begin their journey towards process improvement, they face two very difficult questions: How and where do you start?

This handbook provides an overview of the methodology that we have developed known as “Visible Ops.” Since 2000, we have met with hundreds of IT organizations and identified eight high-performing IT groups with the highest service levels, best security, and best efficiencies. What was most amazing about them was that they shared the following attributes: a culture of change management, a culture of causality, and a culture that fundamentally valued effective and auditable controls, promoting fact-based management. Visible Ops reflects the lessons learned about how these organizations work and describes a control-based entry point into the world of ITIL that others can leverage to springboard their own process improvement efforts.

In the IT industry, Stephen Elliot, an IT Senior Analyst with IDC, showed that on average, 80% of IT system outages are caused by operator and application errors.¹ This motivated our need to dig into causal factors of infrastructure downtime, which continually revealed shortfalls in change management practices. Often, many organizations would have well-documented change management practices, but in reality, no one ever followed them. In many of these cases, the goals and motivations for having change management were not clear to management or to the practitioners themselves. Another key finding was that having a documented change management process was necessary, but far from sufficient, to achieve high-performing characteristics. In the high-performing organizations we studied, change management was embedded in their culture, and had a very different meaning than in typical organizations. This book is dedicated to describing those practices that set the high-performers apart.

Something Must Need Improvement—Otherwise, Why Read This?

“The most likely way the world will be destroyed, most experts agree, is by accident. That’s where we come in; we’re computer professionals. We cause accidents.”—NATHANIEL BORENSTEIN

The motivation for ITIL, change management, and overall process improvement is well known. The trade press is full of stories about cost cutting measures, outsourcing, and regulatory requirements from Sarbanes-Oxley, HIPAA (The Health Insurance Portability and Accountability Act of 1996), BASEL II, FISMA and so forth. The list of people talking about the problems is already large enough, so we promise to keep the discussion of the problem domain to a minimum. In this booklet, the issues and challenges that we address include:

- Organizations have change management processes, but view these processes as overly bureaucratic and diminishing of productivity. There must be more to change management than bureaucracy, good intentions and scarcely attended meetings.
- Organizations where, deep down, everyone knows that people circumvent proper processes because crippling outages, finger-pointing, and phantom changes run rampant.
- A “cowboy culture” where seemingly “nimble” behavior has promoted destructive side effects. The sense of agility is all too often a delusion.
- A “pager culture” where IT operations believes that true control simply is not possible, and that they are doomed to an endless cycle of break/fix triggered by a pager message at late hours of the night.
- An environment where IT operations and security are constantly in a reactive mode, with little ability to figure out how to free themselves from fire-fighting long enough to invest in any proactive work.
- Organizations where both internal and external auditors are on a crusade to find out whether proper controls exist and to push madly for implementing new ones where they are not in place.
- Organizations where IT understands the need for controls, but does not know which controls are needed first.

What You Do And Do Not Need To Know

You do not need an extensive knowledge of ITIL, process improvement, security or audit to benefit from this book. These topics are introduced in this handbook as they become necessary in the Visible Ops methodology. Our intent is to create a working knowledge of critical concepts in these domains, both to serve as a primer and to introduce the language necessary to work with other functional departments, such as security and audit. However, we recognize that each one of these domains is an entire vocation and field of expertise unto itself, so we list recommended resources in the appendices for those wishing to learn more. An evolving list of resources can be found on the ITPI Web site at <http://www.itpi.org>.

Structure Of The Book

This booklet presents information in the following order:

- Visible Ops: What is it and why does it work?
- There are four Visible Ops phases. In each, we describe:
 - Issues and indicators
 - Specific prescriptive steps to solve the issues
 - Benefits and what you are likely to hear as the steps are implemented
- Appendices that provide a brief primer on auditable controls, information on how to proactively prepare for an audit, a summary of ITIL, and other helpful resources.
- In each of the Visible Ops phases, “Helpful Tips When Preparing for an Audit” sections appear in grey call-out boxes, highlighting areas of special interest to those who interact with auditors.

Please note that we use “production” and “operations” interchangeably to specify the team primarily responsible for day-to-day infrastructure operations and maintenance. Specifically, this does not include the release management team. They are in the preproduction portion of the service delivery lifecycle.

¹ Source: Stephen Elliot, Senior Analyst Network and Service Management, IDC, 2004. Note, additional information can also be found from the Gartner Group at http://www4.gartner.com/DisplayDocument?id=334197&ref=g_search

Visible Ops

"It is not enough to show that a situation is bad; it is also necessary to be reasonably certain that the problem has been properly described, fairly certain that the proposed remedy will improve it, and virtually certain that it will not make it worse."—ROBERT CONQUEST

We developed the Visible Ops methodology because everyone seemed to be asking the same urgent question: "I believe in the need for IT process improvement, but where do I start?" There were no satisfactory answers. Although ITIL provides a wealth of best practices, it lacks prescriptive guidance: In what order and how should the practices be implemented? Moreover, the ITIL books remain relatively expensive to distribute widely. The third-party information that is publicly available on ITIL still tends to be too general and vague to effectively aid organizations. This booklet provides step-by-step guidance and a prescriptive roadmap for organizations starting or continuing their IT process improvement journey. Visible Ops uses ITIL terminology, and is intended to be an "on-ramp" to the rest of the ITIL body of knowledge.

History Of Visible Ops

Since early 2000, Gene Kim, CTO of Tripwire, Inc., and Kevin Behr, CTO of IP Services, have studied what contributes to the success of high-performing IT organizations. IP Services is a business process outsourcing company, managing thousands of servers for Fortune 50 organizations. At IP Services, the IT operations group reports to Kevin, and for years, he tried to understand how to best increase service levels and decrease cost to maximize value. Tripwire is a software vendor for a product that detects change—it was originally written by Gene in 1992 as an intrusion detection technology to help system administrators recover from the 1988 Morris Internet Worm. Gene has spent years trying to understand why their largest customers kept insisting that Tripwire's software was not a security technology, but instead, a technology to enforce their change management processes.

Kevin and Gene began working together when they discovered they had a common passion to really understand what differentiated high-performing IT organizations from their more typical counterparts. Visible Ops began to take shape when they started studying a list of organizations that Gene had been keeping for years, which he called "Gene's list of people with amazing kung fu."

After years of research and investigation, Kevin and Gene now refer to this list more formally as "the high performing IT operations and security organizations with the highest service levels, as measured by mean time to repair (MTTR), mean time between failures (MTBF), and availability;² the early integration of security requirements into the operations lifecycle; the lowest amount of unplanned work; and the highest server to system-administrator ratios." What makes the organizations on this list especially astonishing is that they also have more efficient cost structures than lower-performing organizations.

To coordinate and expand their efforts, their works were donated to the Information Technology Process Institute (ITPI). The ITPI is a not-for-profit organization engaged in three principle areas of activity: research, benchmarking and the development of prescriptive guidance for practitioners and business executives. The ITPI has collaboration agreements in place with research organizations such as The University of Oregon Decision Sciences program and The Software Engineering Institute at Carnegie Mellon University. The ITPI also attracts many other contributors through the ITPI Community of Practice List (ICOPL). At the time of writing, there are

² Appendix D is the glossary of terms.

hundreds of top practitioners from IT Operations, Security, Audit, Management, and Governance on the ICOPL, representing thousands of years of IT experience.

Through research, development and benchmarking, the ITPI creates powerful measurement tools, prescriptive adoption methods (such as Visible Ops), and control metrics to facilitate management by fact. The end result of these efforts is to assist organizations with their IT process improvement efforts. This booklet serves as an example.

Common Characteristics Of High-Performing IT Organizations

What makes high-performing organizations so different from average organizations, both qualitatively and quantitatively? We observe that high-performing IT organizations share the following characteristics:

- **Server to system administrator ratios greater than 100:1**—This means that each system administrator controls more than 100 servers. In contrast, organizations not using effective processes see ratios around 15:1.

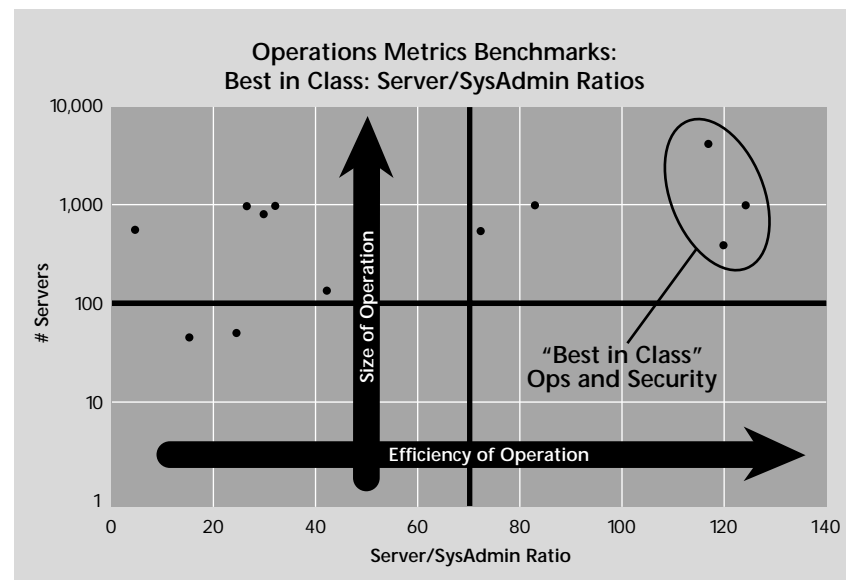


Figure 1: Server to System Administrator Ratio

- **Low ratio of unplanned to planned work**—Only 5% of operational expense goes toward unplanned work. From our ongoing benchmarking, we find that average organizations spend 25–45% of their total operational expenses on unplanned, unscheduled work.
- **Higher staffing early in the IT lifecycle**—Continual deployment of resources and staff in the preproduction build phase, where the cost of defect repair is least expensive.
- **Collaborative working relationships between functions**—IT operations and security work together to solve common objectives, with IT operations performing most of the work and security acting as coach and consultant.
- **Posture of compliance**—Trusted working relationship between IT operations and auditors, because controls are visible, verifiable and regularly reported on.
- **Culture of change management**—Ubiquitous understanding throughout the organization that changes must be managed in order to achieve business objectives.
- **Culture of causality**—Through the use of controls and metrics, these groups identify and solve problems through logical use of cause and effect, instead of a culture of “let’s see if this works.”
- **Management by fact**—These organizations value controls and metrics, not only to aid effective problem solving, but to aid fact-driven decision making, as opposed to “management by belief” or “management by the honor system.”

Why Did We Use ITIL?

To understand what the best in class organizations were doing, Gene and Kevin wanted to determine the union and intersection of their IT processes. In other words, what are the common practices of all the high-performing IT operations organizations studied, and which ones are necessary to achieve the high-performing characteristics? Even this line of questioning was a challenge, because each organization had independently developed their own processes, and each had Darwinistically evolved to learn from past mistakes to prevent certain IT disasters from ever happening again.³ Because they were building their own playbook, as opposed to using an external standard, each organization called similar processes by different names. For example, one organization’s “change management” process was another’s “work authorization request system” or “change control” process. As a result, Kevin and Gene first needed some way to normalize terminology in order to determine what processes these organizations had in common.

To resolve this terminology problem, they did a Google search on “release management and change management,” which brought them to ITIL. ITIL is a compilation of IT best practices, provided without prioritization or any prescriptive structure. ITIL provides a framework and catalog of IT operational processes, distilled from thousands of man-years of experience. Initially created in the late 1980s, the ITIL body of knowledge continues to be enhanced and better organized, most significantly (in our opinion) in the form of the BS 15000, which divides all the ITIL disciplines into five key areas: Release Processes, Control Processes, Resolution Processes, Relationship Processes, and Service Delivery Processes.

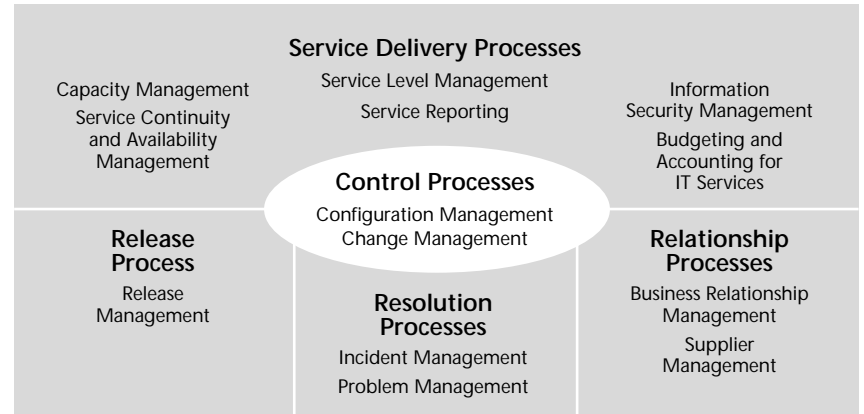


Figure 2: BS 15000 view of ITIL process areas⁴

The BS 15000 categorizes the ITIL capabilities into five areas. Each are briefly described below:

- **Release Process**—This process area answers the question of “where does infrastructure come from before it is deployed?” This includes activities such as the planning, designing, building, and configuring of hardware and software. Unfortunately, release processes are traditionally the last process area that organizations invest in. Yet this is the process area that delivers the highest return on investment, because it encompasses the entire pre-production infrastructure, where the cost of defect repair is lowest.
- **Control Processes**—This process area covers maintaining production infrastructure, not only to prevent service interruptions, but also to efficiently deliver IT service. This is done through change management, as well as asset and configuration management. BS 15000 defines change management as well as asset and configuration management as primary controls. As Stephen Katz, former CISO of Citibank, once said, “Controls don’t slow the business down; like brakes on a car, controls allow you to go faster.”
- **Resolution Processes**—This process area is triggered when production infrastructure does go down, service is interrupted, or there is a security issue. Incident management owns the customer relationship, and problem management owns the tasks of turning each problem into a known error that can be more efficiently resolved the next time it happens. All too often, organizations that spend too much time firefighting are unable to spend time in the previous two process areas.
- **Relationship Processes**—This area focuses on the processes necessary to support effective customer relations as well as the management of third party vendors from a performance and contractual standpoint.
- **Service Delivery Processes**—The goal of these processes is to provide the best possible service levels to meet the business needs of the organization. This process area includes the monitoring and management of IT infrastructure as it relates to Security Management, Availability and Contingency Management, Capacity Management, Financial Management and Service Level Management and Reporting.

³ Similarly, FAA insiders say that “behind every regulation is an airline crash.”

⁴ BS 15000-1:2002—“IT Service Management: Part 1: Specification of Service Management.” British Standards Institute. September 2002. Page 2.

In the high-performing organizations, the common processes were in the release, controls and resolution areas. All of the high-performers had repeatable and verifiable processes to provision infrastructure in a known good state. They had a culture of change management as a primary way to do work and they all used causality in their problem resolution processes. It is interesting to note that none of the high-performing shops were using ITIL at the time of the research. But again, ITIL provided a framework to name and normalize the practices that the high-performing organizations had in common.

ITIL is still not in a form where you can simply distribute the ITIL volumes to your entire IT organization and expect everyone to know what issues to tackle first and what everyone's role should be. Yet experienced IT practitioners who have built their own playbook of lessons and have learned from their own disasters, or near-disasters, are likely to love reading the ITIL volumes. They will see reflections of their own belief systems and management practices in the ITIL, and recognize the wealth of hard-won lessons and processes contributed by other IT practitioners that they can add to their playbook. With these expectations, ITIL can be a tremendous wealth of useful information.⁵

One last note on ITIL: We are continually awed and amazed that so many organizations have re-created the hard-won lessons embodied in ITIL over and over again. Because each of these organizations created their own methodology, when these IT operations organizations meet, even though they are doing very similar things, they cannot speak a common language. One of the first things that a community of practice must develop to share best practices is a common vocabulary. By using ITIL, we normalized the various terms into a standard framework.

In our opinion, just mapping your IT operational processes to ITIL has value. It allows organizations to share best practices plus leverage the tremendous wealth of ITIL and its various advocacy groups, such as the itSMF.⁶ At an even more practical level, being aware of ITIL terminology facilitates interaction with other IT organizations and lowers the risk of misunderstandings.

Why Visible Ops Works

Since 2002, we have presented our research and the Visible Ops methodology to a wide cross-section of the IT community. Through this process, we have received positive feedback from hundreds of people in virtually every industry, company size and functional role. Sometimes we ask ourselves why Visible Ops resonates so well. We now believe that it is because Visible Ops is both logical and intuitive, equally accessible to technical and non-technical stakeholders. Typical reactions are: "This makes so much sense—I have to show this to my boss" and "Wow, our company needs to do this" and even "Visible Ops shows that common sense is rarely common practice."

By replicating how the high-performing IT organizations work, Visible Ops presents practices that not only make sense, but also can be implemented in any organization (i.e. "this really isn't rocket science"). For novice organizations, Visible Ops provides useful guidance on where to start their improvement efforts. For more mature organizations, Visible Ops provides a framework for continual improvement.

⁵ For more information on ITIL, please see Appendix B.

⁶ <http://www.it-smf.com/>

Visible Ops is also accessible to business management, security, and audit because it is controls-based. By being based on controls, not only are regulatory issues addressed, but controls help provide the reliable delivery of IT service. Visible Ops identifies key issues that undermine service levels and security, and provides prescriptive guidance to address them. These issues are:

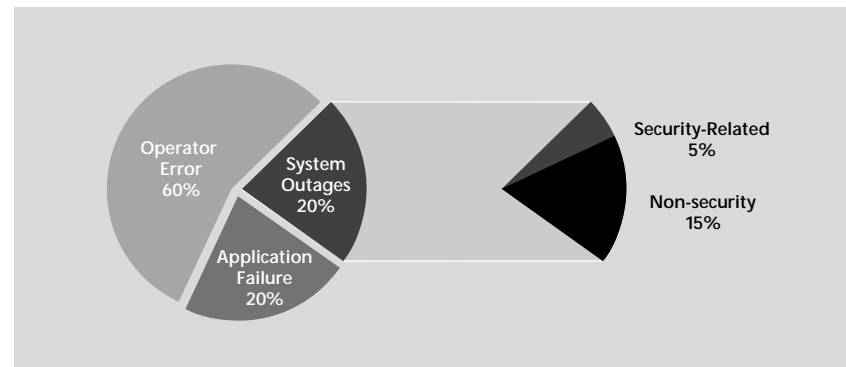


Figure 3: 2004 IDC Study on Causes of Network Downtime⁷

- **Human factors effect successful change**—Implementing a change management process and having it actually followed are two very different things. To meet the requirements of the business, effective change management is a necessity. In order for it to work, human factors must be addressed.
- **80% of outages are self-inflicted**—Donna Scott, VP & Research Director, Gartner, notes that, "80 percent of unplanned downtime is caused by people and process issues, including poor change management practices, while the remainder is caused by technology failures and disasters."⁸
- **80% of MTTR is often wasted on non-productive activities**—Determining the cause of an outage consumes a great deal of valuable time without effective change management. This protracts the outage and makes repair more difficult.
- **Absence of a "culture of causality"**—People often manage and work by intuition and "gut feel." Consequently, they fail to use problem-solving skills and causality to resolve issues. The Microsoft Operations Framework (MOF) study showed that their high-performing customers reboot servers 20 times less often than average and have five times fewer "blue screens of death."
- **Rebuild vs. Repair**—High-performing organizations make it easier to rebuild infrastructure than to repair it. The results are higher and more predictable service levels, plus, by rebuilding from documented standard builds, more junior staff can handle repairs.

⁷ Source: Stephen Elliot, Senior Analyst Network and Service Management, IDC, 2004.

⁸ Miller, David. "Hardware High-Availability Programs in Action. (Product Information)." ENT News. June 1999. <http://www.entmag.com/archives/article.asp?EditorialID=6753>

Visible Ops—Key Characteristics

Visible Ops is neither a death march nor a monumental multi-year undertaking. In fact, we have seen organizations successfully complete the first three phases of Visible Ops in 90 days. The initial part of the methodology is broken down into manageable sub-projects prior to moving into a continuous improvement process. The goal is to create the fewest processes necessary to enable sustaining improvement. To do this, each of these sub-projects has the following characteristics:

- **Definitive Projects**—Each phase is a project with a clearly defined objective.
- **Ordered**—Each phase is specifically designed to build upon the previous phase.
- **Catalytic**—Each phase returns more resources to the organization than it consumed, thus fueling the next phase.
- **Auditable**—Each phase creates auditable processes that generate on-going documentation in order to prove controls are working and effective.
- **Sustaining**—Each phase creates enough value to the organization that the processes developed remain in place, even if the initial driving forces behind its implementation disappear.

This approach has many benefits. First, because of the relatively short length of each phase, concepts and their benefits are proven faster. Second, getting executive sponsorship and funding for four smaller phases is easier than for a big vision with a distant promised payoff.

Facilitating A Productive Working Relationship Between IT Operations, Security And Audit

All too often, IT operations groups have an unproductive working relationship with security and audit. Visible Ops creates a framework that creates productive interfaces between these groups, through repeatable, verifiable and auditable IT processes. By exposing IT controls and acceptance points, security and audit are able to review changes before they are implemented, and detect when these controls are circumvented. These controls are used not just to avoid circumstances which can lead to security incidents or unplanned work, but they also allow the continual monitoring and reduction of variance.

Bill Shinn, a System Security Engineer with a Fortune 100 financial institution, has studied the correlation between the amount of unplanned work and the number of security incidents. He has observed that as the number of unplanned changes increases, the likelihood of insecure configurations increases correspondingly, as do the number of incidents where security must investigate issues. For example, security may be called upon during a network outage because the issue is obviously “another firewall problem” instead of an undocumented change made by the network administrators. In contrast, when changes are planned, security has a chance to review, approve and respond to the changes early in the production lifecycle and can route issues to the responsible parties. This early involvement increases the overall IT organization’s ability to fix systemic issues that lead to unnecessary firefighting and security problems.

Similarly, IT auditors often are exasperated by the absence of documented processes, the lack of a defined desired state, and an inability to attest to whether or not the current state meets the documented control objectives. Without these, auditors are unable to determine if risks and controls are in balance. In the absence of verifiable controls, they must go into “archaeology”

mode and make a judgment on whether a material risk exists or not. This is not to say that the IT operations group is necessarily doing a poor job. Indeed, if the staff turnover is sufficiently low, the “tribal knowledge,” or combined team knowledge, can compensate for a lack of formally documented processes, observes Ron Zika, a Senior Consultant for Waypoint, Inc. Visible Ops creates the instrumentation where auditors can review the processes and controls for effectiveness without having to enter into a forensics analysis mode. This leads to a more productive working relationship, smoother audits and less time spent on audit preparation and remediation.

Although IT operations, security and audit have very different roles, the three groups are often needlessly at odds because of the lack of effective controls. By improving processes and controls, all parties benefit by creating a more productive working relationship and allowing the groups to more efficiently achieve common business objectives. How this is done will be covered in more depth later in the book.

An Overview Of The Four Visible Ops Phases

Visible Ops gives organizations a means to begin their process improvement journey. After studying the high-performing organizations, we focused the methodology on four key phases:

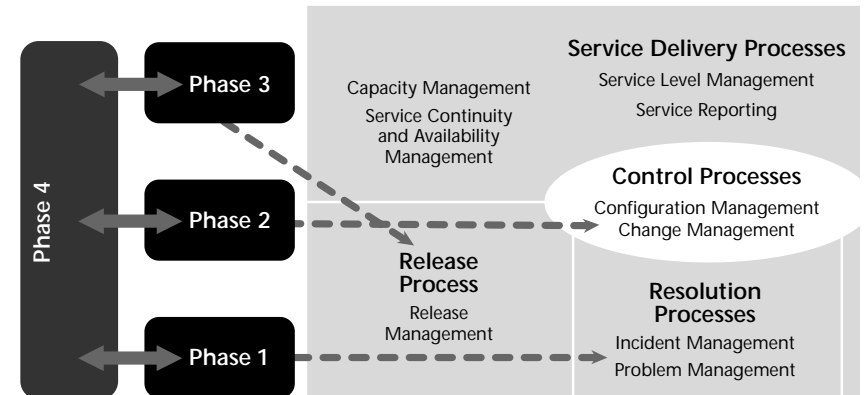


Figure 4: Visible Ops’ Four Phases and Relevant ITIL Process Areas

- **Phase 1: “Stabilize the Patient”**—In this phase, we curb the number of outages by freezing change outside of scheduled maintenance windows. We also modify the first response process of problem managers by ensuring that they have all change related information at hand about what could have caused the outage.
- **Phase 2: “Catch & Release” and “Find Fragile Artifacts”**—Often, infrastructure exists that cannot be repeatedly replicated. In this step, we inventory assets, configurations and services to identify those with the lowest change success rates, highest MTTR, and highest business downtime costs. Fragile artifacts are identified and then treated with extra caution to avert risky changes and massive episodes of unplanned work.