Sustainable Compliance

Toward a value-driven, technology-enabled approach

Version control

Version	Date	Short description changes
0.1	November 13, 2006	Start Report
0.2	November 29, 2006	Revisions by Gerard and table insert by Tina
1.0	November 29, 2006	

Name author(s):
Marco Plas
Tina Rogers
Gerard Verstegen

Sustainable Compliance

Name author(s):
Marco Plas
Tina Rogers
Gerard Verstegen

Company name:	Capgemini Nederland B.V.
Place:	Utrecht
Date:	November 29, 2006

Preface / Introduction

Regulatory compliance is a major challenge for many companies, requiring significant investments and consuming considerable time of staff and management on an ongoing basis.

This white paper addresses a number of key questions regarding regulatory compliance, including:

- what is it?

- why should you care?

- what can you do about it?

- how can ProCurve's solution set and ProActive Defense strategy support you?

Our vision, as described in this paper, is based on the concept of sustainable compliance[1], articulating the idea that compliance initiatives

- should be aiming to attain concrete business benefits in addition to merely meeting minimal compliance requirements – they should be *value driven*; and
- they should fully leverage the possibilities of information technology to meet compliance requirements through automated controls, rendering a preventive, cost-effective way of working that minimizes the burden for employees – they should be *technology enabled*.

This white paper might be relevant for any organisation facing regulatory compliance, and it is written for both management and executives from supporting departments (e.g., from finance & control, compliance, risk management, IT, information security) that have responsibilities related to regulatory compliance.

[1] This concept is derived from the Point of View of Capgemini

Table of Contents

1.1 The challenge of compliance 1
1.2 Regulatory landscape 2
SOX 404 Compliance: basic process 5
2.1 Objectives and ambition 7
2.2 Compliance architecture 8
GRC Foundation 9
Risk & Control Processes 9
Technology 10
4.1 Overview of the ProCurve suite of management software 17
4.2 Compliance reporting 17
4.3 ProCurve ProActive Defense Strategy for regulatory compliance 18

1 Sustainable compliance

1.1 The challenge of compliance

For many companies the challenge to comply with new legislative requirements, such as Sarbanes-Oxley (SOX), Basel II and Markets in Financial Instruments Directive (MiFID), is a major concern. These concerns are primarily driven by the fact that:

- The amount and complexity of new regulations that requires a company to be *in control* has increased rapidly;
- These new regulations require *transparency*. You have to be *visibly* in control and be able to prove this to the outside world. This requires a significant amount of additional and time-consuming documentation to gather evidence;
- Supervision of compliance is strict and the penalties for non-compliance are severe. As such, non-compliance is no longer an option.

Typical questions a company has to address include how to control compliance costs, how to maintain middle-management commitment, how to develop the competencies and expertise required from all employees involved and how to prevent bureaucracy frustrating daily operations.

For a growing number of companies an underlying key question regarding new and existing compliance initiatives is, what is our *ambition*? The projects, processes and systems focusing on compliance require huge investments – amounting to hundreds of millions euros annually for organisations such as banks. Should the only objective of these initiatives be *pure compliance*, aimed at survival, or should an organisation also aim at realising significant business benefits?

1.2 Regulatory landscape

Some of the more important regulations are listed in the table below. Regulations exist for different market sectors, for different business functions and for different parts of the globe. The table bellow lists ten of the regulations that have a high impact on the market. In no particular order, these are:

Regulation	Description	Region
SOX	Sarbanes-Oxley Act *SOX, also known as the Public Company Accounting Reform and Investor Protection Act of 2002, is a United States federal law passed in response to a number of major corporate and accounting scandals. The most important part of the SOX act requires companies to prove they have an effective internal control system.*	US
GLBA	Gramm-Leach-Bliley Act *GLBA, also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.*	US
HIPAA	Health Insurance Portability and Accountability Act *The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a federal statute that provides for the development of uniform national health information data standards and privacy standards.*	US
USA Patriot Act	Act for Providing Appropriate Tools Required to Intercept and Obstruct Terrorism *The Patriot Act was formed in response to the terrorist attacks against the United States, and dramatically expanded the authority of American law enforcement for the stated purpose of fighting terrorism in the United States and abroad.*	US
FDA	American Food and Drug Administration / 21 CFR 11 *The FDA regulations are responsible for regulating food (for humans and animals), dietary*	US

	supplements, drugs (for humans and animals), cosmetics, medical devices (for humans and animals) and radiation-emitting devices (including non-medical devices), biologics and blood products in the United States.	
CDD /KYC	Customer Due Diligence / Know Your Customer standards (as set out by BIS) *CDD states that supervisors around the world need to recognise the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of those controls. Without this due diligence banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.*	International
CIPA	Children's Internet Protection Act *CIPA is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers.*	US
CISP	VISA Cardholder Information Security Program *CISP is a program established by Visa USA to ensure the security of cardholder information as it is being processed and stored by merchants and service providers.*	US
FFIEC	The Federal Financial Institutions Examination Council Authentication in an Internet banking environment guidance *The guidance focuses on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services.*	US
FISMA	Federal Information Security Management Act *FISMA requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or other source.*	US

Basel II	Basel II Agreement for International Convergence of Capital Management and Capital Standards *Basel II lays down new guidelines for determining the minimum solvency requirements for banks. The objective is to improve the soundness of the financial system.*	International
Solvency II	Solvency II Directive *Solvency II Directive imposes quantitative solvency requirements based on insurance risk. It also considers the overall management of risks and the structure of insurance supervision. Solvency II will encompass every aspect of insurance operations.*	EU
AML	Anti-Money Laundering 3rd Directive *The goal of the directive is the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The directive applies to the financial and other key services sectors and also covers all providers of goods, when payments are made in cash in excess of €15.000.*	EU
IFRS	International Financial Reporting Standards *IFRS are a set of accounting standards issued by the International Accounting Standards Board (IASB).*	EU
DPD	Data Protection Directive *This directive protects the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.*	EU

One of the regulations that has had a high, global impact on almost all industries is the Sarbanes Oxley Act, especially the section 404.

Sarbanes Oxley in brief

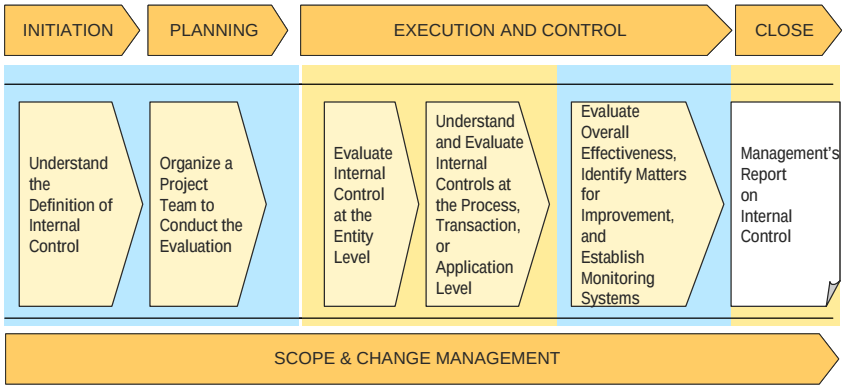
For any U.S.-listed company, the starting point for SOX compliance is the Sarbanes-Oxley Act of 2002, the subsequent guidance issued in 2005 and later. Some background information regarding this act is included in appendix A.2. Whether you are a U.S. Accelerated Filer (AF) or a U.S.-listed Foreign Private Issuer (FPI), the regulations and guidance of the SEC and PCAOB with regard to Internal Control over Financial Reporting (IC/FR) are leading. Section 404 of the SOX Act has the largest impact on the SOX efforts of companies because it requires the substantial effort of re-evaluating the effectiveness of IC/FR each year. However, other sections

also need to be considered, such as Section 302, which requires quarterly reporting of significant changes in internal controls over financial reporting, and sections on whistle blowing, etc.

SOX 404 Compliance: basic process

To achieve SOX 404 compliance, companies typically follow a process of documentation and evaluation as illustrated in Figure 1.

Figure 1. Basic process for SOX 404 compliance



The core of this process focuses on documenting and evaluating the Internal Control on three organisation levels:

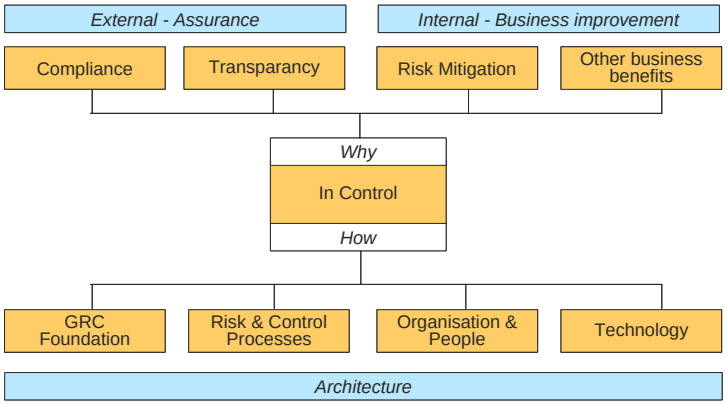
- *Entity and Company Level Controls (ELC), which are typically controls above the process level, can often be leveraged to limit the amount of testing at the process level (see risk-based approach below).*
- *Transaction and Process Level Controls (TLC), which may consist of Manual, IT Dependent Manual and Automated controls.*
- *IT General Controls (ITGC), which are required to control the IT environment for reliable Automated and IT-Dependent Manual controls. Note: IT General Controls are often addressed through models such as CobiT, for which a separate set of software tools is available on the market.*

2 Sustainable Compliance – a framework

Before introducing a tool that might help realise this ambition, a company should consider rethinking its compliance strategy – not only as a base for defining requirements for such a tool, but possibly also as a starting point for a number of other initiatives in areas such as governance, technology, etc.

The framework described here covers the area nowadays labelled as Governance Risk & Compliance, or GRC, and can be applied as a basic structure to design a strategy for sustainable compliance.

Figure 2. Framework for Sustainable Compliance



Developing a compliance strategy using this basic framework has the following advantages:

- Compliance initiatives will be based on a business case.
- Explicitly defined objectives (the ambition level, described at the top of the framework) drive the compliance program and the actual design of the compliance architecture (bottom of the framework).
- It allows for strategic instead of tactical solutions, hence avoiding development of isolated, often temporary solutions.
- It creates insight into the coherence between the individual functionalities and choices regarding, e.g., central versus local governance and technology, including the choice for compliance tooling.

The framework is not centred around compliance but around *control*. The definition of control is taken from the COSO model for Internal Control[2]: '*Internal control is a process, effected by an entity's board of directors, management and other personne, designed to provide* ***reasonable assurance*** *regarding the achievement of objectives.*'

'Control' focuses on 'reasonable assurance', not on *complete* assurance, that objectives are met. In order to identify which controls have to be in place to generate this reasonable assurance, the *risks* that may frustrate accomplishing the defined objectives have to be identified and assessed.

The framework addresses two questions: 1) The *Why:* what *objectives* do you want to accomplish, what's your *ambition*, when initiating a major investment in compliance and control? And, 2) The *How:* what key choices are made that form the base of your compliance architecture?

In the next two sections the *why* – objectives and ambition – and the *how* – architecture – of the framework are further explained.

2.1 Objectives and ambition

Two main sets of objectives are distinguished: rendering *assurance,* or trust, to the outside world, which is externally oriented, and *business improvement*, which is internally oriented.

External objectives - assurance

Assurance is rendered in the form of an In Control Statement (e.g., for SOX) or another reporting form to the regulatory supervisor, e.g., in the case of Basel II. Nowadays nearly all major control initiatives are initiated as a direct consequence of new regulations: compliance is the primary objective.

One characteristic many new regulations such as SOX, Basel II and Solvency have in common is that they all require your company to be *visibly in control*. This means you have to provide *evidence* to the auditor or supervisor that *proves* you are in control. The required processes of defining, creating, collecting and recording this evidence is one of the key factors driving up compliance costs. Compliance tools are designed to help streamline and support these processes.

A complication faced by many companies, not only in the finance industry, is that they have to simultaneously comply with not one but an array of regulations and policies, each leading to a separate set of requirements for a unit or department. Consequently a unit manager has to:

- Implement several different control systems, which partly overlap;

[2] Committee of Sponsoring Organizations of the Treadway Commission, 1994: '*Internal Control – Integrated Framework*'

- Report on compliance to different corporate functions;
- Capture and provide different evidence sets.

This may lead to major inefficiencies and has triggered a growing number of companies to consider an alternative for the isolated (regulation-by-regulation) approach that is applied in most cases. This alternative, an *integrated approach*, ideally leads to one, integrated risk and control framework. This integrated framework comprises all relevant regulations and policies and is based on one integrated documentation set of business processes, risks and controls**.**
Besides compliance, *transparency* is defined as the second objective. Transparency here is used to indicate the situation where a company *voluntarily* chooses to render assurance through an In Control Statement, thereby satisfying the growing demand from stakeholders for transparency. An example of this is Rabobank, a Dutch bank, which decided to become SOX compliant, with no legal obligation to do so.

Internal objectives – business improvement

For business improvement two categories are identified: risk mitigation, which is the direct objective of control, and other business benefits. Risk mitigation leads to a reduction of errors and thus subsequently to a reduction of error costs and often to a higher service level.

An example of other benefits is the simplification and streamlining of business processes. Before looking at the *control* of a process, it may be wise to assess the *controllability* of that process. When different business units for a certain process (for example client acceptance) have different variations in place, some simple and some complex, streamlining these processes will not only be a beneficial step in itself, it will also simplify the control requirements and reduce control costs.

Ambition

Given this set of possible objectives a key question for a company is, what is the ambition level that drives my compliance strategy?

2.2 Compliance architecture

The previous section focused on objectives and ambition,\; now we examine how these ambitions can be realised.

Within a compliance architecture, we distinguish four main areas:

- GRC Foundation;
- Risk & Control Processes,
  captured in a number of GRC domains, see figure 3;
- Organisation & People;
- Technology.

For each area some key choices are discussed. These choices lead to the business principles that form the base of a compliance architecture.

GRC Foundation
The GRC Foundation relates to a number of basic conditions that have to be met for most GRC domains, including a process model, with documented processes, a documented organisational model and a strategy for communications.

Two examples of key choices that are often relevant are:

- Streamlining of processes:
  To what extent are redesigned activities (to simplify and streamline business processes, undoubtedly with impact on the supporting information systems) included in the overall compliance efforts? The choice will depend largely on opportunities for improvement and feasibility, together with the level of ambition.
- Documentation strategy:
  To what extent are processes documented (for SOX documenting processes is one of the controls and part of the required evidence), to what extent are the same standards and methodology used corporate wide and to what extent is all documentation recorded in a single repository and accessible by the same tool.

Risk & Control Processes
The actual content of the Risk & Control Processes will, to a large extent, differ by GRC domain. For each domain four generic groups of activities can be distinguished, focusing on

- Risk assessment;
- Prevention,
  including controls such as policies and standards, automated controls, training;
- Detection and assurance,
  including controls such as self assessments, internal reporting;
- Response ,
  including controls such as remediation, incident management.

One overall key choice, mentioned before, relates to the level of integration between the different GRC domains. To what extent can preventive controls and activities for detection and for assurance be shared? What benefits in terms of quality and efficiency can be gained? What impact will these choices have for organisational responsibilities and for supporting tools?
Organisation and people

Three important choices here are the following:

- *Governance: Top down versus bottom up*
  This relates to the level of autonomy that local units and divisions have in realising the objectives and principles defined at corporate level. Choices here may differ for the various GRC domains. Some considerations are summarised.

- *Accountability*
  This area relates to the way responsibilities and authorisations are distributed:
  - Between line and supporting staff;
  - Between the different supporting staff functions (e.g., Risk Officers, Compliance Officers, Finance & Control, Internal Auditor);
  - Between corporate and local level.

  Lack of clarity in this area is not uncommon and can strongly frustrate progress in other areas.

- *Organisational embedding*
  The question here is, to what extent do you invest in a *culture* where commitment to control and compliance is common (the 'control environment' of the COSO model) and the development of *competencies and expertise* required for staff at all levels to be able to act and bear responsibilities according to the rules that are set?

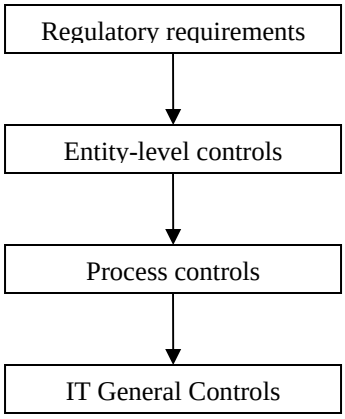
Technology

One of the most valuable assets of any organisation is information. As organisations become more dependent on technology to harvest this information, it becomes progressively important to control the technology.

Many of the regulations aim to support this objective but seem to contradict the desire of organisations to operate in a more flexible manner with suppliers, clients and tele-working staff. Organisations tend to find themselves in a continuous balancing act between flexible interoperability and the need to be compliant with regulations.

These regulations have requirements that enforce an effective working and control of an organisation. Often they define the controls that need to be in place in an organisation.

For example, for SOX 404 controls have to be in place at three levels, as shown in the figure below. Process controls typically involve applications controls. As a consequence, the related application must be embedded in a reliable IT environment.



IT General Controls (ITGC) form the foundation of a controlled IT environment. The most comprehensive and internationally adopted control framework for IT is COBIT. The COBIT framework consists of 215 control objectives within 34 high-level objectives, brought together in four manageable groups. If implemented and managed correctly, this framework delivers strong governance and control over the IT environment while maintaining flexibility and accountability.

Technology is often not only an *object* but also an *enabler* of compliance. For example, for the following two areas:

- *Automated controls versus manual controls*
  Experiences after the first year of SOX 404 implementations in the U.S. showed that 75 % of SOX statements were based on manual controls and only 25 % on automated controls. The advantages of automated controls are evident: they are preventive, more efficient and more reliable. For many companies this is a major improvement opportunity. Extending the level of automated controls brings about a reduction in costs and an improvement in the quality of operational processes.
- *Automated testing & monitoring*
  In the event that controls are automated, a growing number of tools can decrease the testing effort through *automated testing* facilities. There are, for example, tools that automatically analyse the existence and actual operational effectiveness of segregation of duties, which not only saves time but also improves the effectiveness of testing.

  One step beyond automated testing is *continuous monitoring*, which relates to a facility that;

  - monitors all business transactions processed in an application,
  - identifies anomalies (based on self-defined rules, e.g., two occurrences of exactly the same purchase order in one day should be labelled as a possible anomaly) and

- reports on the outcome, bringing internal control to a new, higher level.

The question here is, do you want to include these kinds of improvement steps in the compliance program?

3 IT Governance and Information Security - a cornerstone of regulatory compliance

As discussed in the previous chapter, IT General Controls form a strong basis for controlling information assets within the organisation, thus providing stronger IT governance. A solid control framework for IT is an absolute necessity for achieving regulatory compliance.

The Information Systems Audit and Control Association (ISACA) promotes the use of COBIT as the standard for IT governance and control.

COBIT provides benefits to managers, IT users and auditors. Managers benefit from COBIT because it provides them with a foundation upon which IT-related decisions and investments can be based. Decision making is more effective because COBIT aids management in defining a strategic IT plan, defining the information architecture, acquiring the necessary IT hardware and software to execute an IT strategy, ensuring continuous service, and monitoring the performance of the IT system. IT users benefit from COBIT because of the assurance provided to them if the applications that aid in the gathering, processing and reporting of information comply with COBIT, because it implies that controls and security are in place to govern the processes. COBIT benefits auditors because it helps them identify IT control issues within a company's IT infrastructure. It also helps them corroborate their audit findings.

COBIT covers four domains:

- Plan and Organise
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

The first two domains relate more to the process-level control and deal with the planning and implementing phase. The last two domains deal more with the IT general controls and relate strongly to capabilities of the ProCurve management suite. The management and reporting capabilities of the ProCurve management suite have been designed in such a way that they fully map to the CobiT 4.0 control objectives in these last two domains.

Plan and organise

The Planning and Organisation domain covers the use of technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organisational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT.

Acquire and implement

This domain encompasses identifying the company's IT requirements, acquiring the technology and implementing it within the company's current business processes. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT system and its components.

Delivery and Support

The Delivery and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results, as well as the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training. The following table lists the high-level control objectives for the Delivery and Support domain.

HIGH-LEVEL CONTROL OBJECTIVES

Deliver and Support

DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

Monitor and Evaluate

The Monitoring and Evaluation domain deals with a company's strategy in assessing the needs of the company and whether or not the current IT system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of an IT system in its ability to meet business objectives and the company's control processes by internal and external auditors. The following table lists the high-level control objectives for the Monitoring and Evaluation domain.

HIGH-LEVEL CONTROL OBJECTIVES

Monitor and Evaluate

ME1	Monitor and Evaluate IT Processes
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

COBIT's relation to ProCurve

The COBIT model comprises a total of 215 control objectives, grouped together in 34 high-level control objectives. The table below indicates where ProCurve reports and capabilities can help an organisation to achieve a level of control that is needed for regulatory compliance.

COBIT DOMAIN	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Plan and Organise													
Acquire and Implement													

Deliver and Support	Define and Manage Service Levels	Manage Third-party Services	Manage Performance and Capacity	Ensure Continuous Service	Ensure Systems Security	Identify and Allocate Costs	Educate and Train Users	Manage Service Desk and Incidents	Manage the Configuration	Manage Problems	Manage Data	Manage the Physical Environment	Manage Operations
Monitor and Evaluate	Monitor and Evaluate IT Processes	Monitor and Evaluate Internal Control	Ensure Regulatory Compliance	Provide IT Governance									

N/A (no controls)

Direct ProCurve domain mapping

Indirect or no ProCurve domain mapping

4 ProCurve Networking by HP's solution set as enabler for regulatory compliance

4.1 Overview of the ProCurve suite of management software

The ProCurve suite of management software consists of the following products:

- ProCurve Manager Plus (PCM+) switch management software
- Identity Driven Manager (IDM) access control software
- Network Immunity Manager (NIM) internal threat detection and response software

These software management tools provide network management security such as security management protocols, device authentication, management access control, user access control and monitoring the network for internal threats such as virus attacks. They have been designed with regulatory compliance in mind.

4.2 Compliance reporting

A strong reporting portfolio offers the necessary proof of control over the IT infrastructure will assist IT staff in making proper evaluations of the network and will assist auditors in the gathering of evidence. Reports from the ProCurve solution suite have been created in such a way that they relate directly to control objectives from the COBIT control framework. Additional reports are created as a benefit to system administrators.

The ProCurve solution suite offers a comprehensive set of reports to:

- Effectively manage the network infrastructure;
- Assist customers with regulatory compliance; and
- Ensure and enhance IT governance.

The following is a partial list of ProCurve software management reports planned for availability in Summer 2007 that are recommended to assist with regulatory compliance:

ProCurve Manager Plus Reports

- Device Security History Report
- Device Access Security Report
- Port Access Security Report
- Password Policy Compliance
- Current credentials Report

Network Immunity Manger Reports

- Security Policy Action Report
- Security Events History Report
- Security Heat Map Report
- Offenders Tracking Report

Identify Driven Manager Reports

- User Unsuccessful Login Report
- User Session History
- User MAC address Report

For a full list of reports planned for availability in Summer 2007, please refer to the list of reports posted at *www.procurve.com/security*.

4.3 ProCurve ProActive Defense Strategy for regulatory compliance

ProCurve's security strategy is called ProCurve ProActive Defense.

The ProActive piece of the strategy is to prevent problems by controlling access to the network at the network edge, including use of the Identity Driven Manager software.

The Defensive piece of the strategy is to secure the network infrastructure by using secure management protocols and device authentication, including use of ProCurve Manager Plus software, and to monitor behavior on the network to make the network resilient to attacks by providing internal threat detection and response solutions such as the Network Immunity Manager software.

With these security solutions, ProCurve provides robust security at the edge of the network, where users and devices connect. These management tools help control and monitor the network infrastructure to assist IT administrators with regulatory compliance.

About Capgemini and the Collaborative Business Experience

Capgemini, one of the world's foremost providers of Consulting, Technology and Outsourcing services, has a unique way of working with its clients, called the Collaborative Business Experience.

Backed by over three decades of industry and service experience, the Collaborative Business Experience is designed to help our clients achieve better, faster, more sustainable results through seamless access to our network of world-leading technology partners and collaboration-focused methods and tools. Through commitment to mutual success and the achievement of tangible value, we help businesses implement growth strategies, leverage technology and thrive through the power of collaboration. Capgemini employs approximately 61,000 people worldwide and reported 2005 global revenues of 6,954 million euros.

The Capgemini Group is headquartered in Paris.

www.capgemini.com

About ProCurve Networking by HP

The ProCurve Networking business unit of HP delivers enterprise networking solutions comprising wired and wireless LAN and WAN networking products, services and solutions. Recognizing the necessary migration of intelligence and functionality to the network edge, the ProCurve Adaptive EDGE Architecture strategy is the industry's only comprehensive and inclusive network design strategy that is adaptable, scalable and completely interoperable for achieving command from the center with control to the network edge. ProCurve was positioned in the challenger quadrant in research and advisory firm Gartner, Inc.'s 2006 Magic Quadrant Report for Global Campus LANs.

Further information on ProCurve networking solutions and products is available at www.procurve.com.

About HP

HP is a technology solutions provider to consumers, businesses and institutions globally. The company's offerings span IT infrastructure, global services, business and home computing, and imaging and printing. For the four fiscal quarters ended Oct. 31, 2006, HP revenue totaled US$91.7 billion. More information about HP (NYSE, Nasdaq: HPQ) is available at www.hp.com.