**THIS PUBLICATION CONSISTS OF TWO SECTIONS**

**A) REPORT**

**B) PRESENTATION**

# Introducing Security at the Cradle, Not the Grave
## SANS Audit and  Security Controls that Work
## Jennifer Bayuk
## April 6, 2003

It is the role of IT to provide systems and processes to facilitate business operations.  You may argue there are exceptions in the cases where the business is IT.  But even then, there is some aspect of operations which is the books and records of the firm, and that is operating the business, not operating IT.  IT does not operate the business.  IT operates systems.

Given that IT's role is to facilitate, not to operate, deference is always given to those who do operate, that is, the money makers.  A good CIO is one who provides the money makers with the IT tools and techniques they need to run the business.  Many money-makers avoid coming to IT, preferring to make money with the tools and techniques with which they are already familiar,  but some recognize the competitive advantage that leading edge IT can provide. So when a money-maker asks for a given application or function, a good CIO tries to oblige.

The same could be said of a corporate airplane pilot.  When the money-maker needs to travel to close a deal, the corporate pilot will always chart a course.  However, if the money-maker wants to fly through the mountains of Montana in a storm, it is the role of the pilot to advise against, and sometimes even to refuse to steer, given that there is too much personal risk in the process.  Similarly, it is the role of the CIO to caution and sometimes to refuse a risky request.

The analogy continues.  Just as it is the role of the FAA to create rules that allow pilots to safely operate despite business pressure to take off, it is the function of IT Security to give some credence to the IT risk management function.

I once worked on expert systems for Air Traffic Control simulation and training.  It was common knowledge that behind every rule from the FAA, there is a plane crash.  For example, detailed rules concerning de-icing wings were placed on the books shortly after the root cause of a plane crash was found to be ice on a wing.  The fact that the crash happened made the rule enforceable, and it elicited recognition from the airlines that the rule made sense to enforce.

In IT Security, the recognition is not so common because the crashes don't usually make the news.  But behind every computer security standard is an incident.  The incident is not always a crash.  More commonly, it is fraud.  For many computer security rules, such as authentication, the knowledge of what could happen without the rule make the rule obvious.  But overall, no rulebook in computer security is as black and white as that of the FAA.

# Introducing Security in the Cradle

**Jennifer L. Bayuk**
**jbayuk@bear.com**

**SANS Audit and Security Controls that Work**
**April 6, 2003**

BEAR
STEARNS

# The Role of IT

- **Money Makers Operate the Business**

- **Money Makers Fund IT to Design and Operate IT**

# A CIO is like a Corporate Pilot

- Money Makers exert pressure
- Rulebooks provide comfort level for safe decisions
- Risk Managers provide much needed checkpoints

# Easy proof for Risk Managers

**Axiom 1:** **Management must control assets and resources.**

**Axiom 2:** **Computers control assets and resources.**

**Theorem:** **Management must control computers.**

# Security is not omnipotent

**Axiom 3:** **Those who administer systems to some extent control them.**

**Axiom 4:** **All systems are controlled to some extent by people whose job function is not security.**

# Security cannot be omnipotent

**Axiom 5:** **It is not true that all systems are controlled to some extent by people whose job function is not security.**

**Given the job functions of data transfer, performance tuning, and batch job scheduling, two possible conclusions:**

- **Axiom 5 is false**
- **security administration is part of the job function of others who touch the machine**

# Security is already distributed

IT Management exists

CIO delegation of authority exists

Organizational processes exist

Security controls should align with the processes that run IT

# Commonalities in IT Processes

Key Goal Indicators

Key Performance Indicators

Level of Maturity

Level of Commitment

# Examples of IT Processes (COBIT)

***Planning & Organization***

Define a strategic IT plan
Define the information architecture
Determine the technological direction
Define the IT organization and relationships

P05

**Manage the IT investment**

Communicate management aims and direction
Manage human resources
Ensure compliance with external requirements
Assess risks
Manage projects
Manage quality

***Acquisition & Implementation***

Identify solutions
Acquire and maintain application software
Acquire and maintain technology architecture
Develop and maintain IT procedures
Install and accredit systems
Manage changes

***Delivery & Support***

Identify solutions
Acquire and maintain application software
Acquire and maintain technology architecture
Develop and maintain IT procedures
Install and accredit systems
Manage changes
Define service levels
Manage third-party services
Manage performance and capacity
Ensure continuous service
Ensure systems security
Identify and attribute costs
Educate and train users
Assist and advise IT customers
Manage the configuration
Manage problems and incidents
Manage data
Manage facilities
Manage operations

***Monitoring***

Monitor the processes
Assess internal control adequacy
Obtain independent assurance
Provide for independent audit

# P05 Key Goal Indicators

- Percent of IT investments meeting or exceeding expected benefits, based on return on investment and user satisfaction
- Actual IT expenses as percent of total organisation expenses vs. target
- Actual IT expenses as a percent of revenues vs. target
- Percent of business owner IT budgets met
- Absence of project delays caused by lags in investment decisions or unavailablity of funding

# P05 Key Performance Indicators

- **Percent of projects with business owners**
- **Months since last review of budgets**
- **Time lag between deviation occurrence and reporting**
- **Percent of project files containing investment evaluations**
- **Number of projects where business benefits are not verified post-facto**
- **Number of projects revealing investment or resource conflicts after approval**
- **Number of instances and time-lag in delayed use of new technology**

# Security Maps to IT Process

- Returns on investment may not be met if the costs of implementing security requirements are not considered
- Security concerns of users, third parties, or internal data owners may cause project delays
- New technology may introduce unexpected infrastructure vulnerabilities that create resource conflicts

# Example – New Desktop Request

- User requests desktop program from dedicated desktop admin
- Admin checks “approved” list, requested program is not there
- Admin advises user to make formal request through software acquisition process
- Software acquisition process requires desktop engineering approval
- Control point within desktop engineering approval is “security review”
- Security Reviews request, bringing admin and/or back for configuration consultation if required

# The Role of IT Security

**Prevention:** Security standards and assignment of formal accountability for compliance

**Detection:** Monitor compliance

**Recovery:** Investigate incidents and arbitrate policy exceptions

# Focus on Process Integration

- Minimizes need for dedicated security staff
- Leverages platform administrator expertise for security goals
- Allows IT Security to concentrate on architecture and monitoring

# Security Performance Indicators

- Policy is clear for all platforms and standards are clear for platforms where risk levels are high or distributed administration is prevalent
- Security review and approval is part of the System Software and Architecture Lifecycle, especially with respect to security software selection and configuration, and new network connectivity
- Configuration change control is monitored
- User administration processes are controlled
- Security incidents are investigated

# An exercise for the reader

**Theorem: Management must control computers.**

**Theorem: Security helps control computers.**

**Corollary: Security helps management.**

# Introducing Security in the Cradle

Jennifer L. Bayuk
jbayuk@bear.com

SANS Audit and Security Controls that Work
April 6, 2003

BEAR
STEARNS

The role of the CISO is akin to the role of the airline safety official. Good pilots do not want to fly in hazardous conditions, and it is up to the airline safety officer to give them checkpoints and decision points, to monitor compliance with the rulebook, and to defend them when they make no-go decisions.

If there is one takeaway I will leave you with – it is this – IT Management, every bit as much as the airline pilot, wants to be in control. They understand the consequences of accidents, and never want to be in a position of responsibility for one. The key to effective security is the recognition on the part of IT Management that security provides control.

This proof is easy to sell:

Axiom 1: Management must control assets and resources.
Axiom 2: Computers control assets and resources.
Theorem: Management must control computers.

Almost anyone would agree with Axiom 3 as well:

Axiom 3: Those who administer systems to some extent control them.

I am going to step through a formal definition of this Axiom for those who like to see this sort of thing laid out in logical detail. Those who do not should skip to the next Axiom:

Definition: C(X,Y) = “X exerts some control over Y”
Definition: A(X,Y) = “X performs actions that affect the ability to control Y
Pseudo Code: For all X, If X performs actions that affect the ability to control Y then X exerts some control over Y
Formal Logic: $\forall (X,Y)\ \ A(X,Y) \Rightarrow\ C(X,Y)$

Axiom 4 is a harder sell. People who have set up elaborate access control systems disagree. However, I sell this statement on the premise that access control is based on job function and non-security people have to have enough access to get their jobs done.

Axiom 4: All systems are controlled to some extent by people whose job function is not security.

Again, the formal logical may be skipped without loss of continuity.

Definition: S = System
Definition: SA = Security Administrator
Pseudo Code: For all X, if X is a system then there exists a Y such that Y is a not the security administrator and Y performs actions that affect the ability to control X
Formal Logic: $\forall (X)\ (\ \ (X == S)\ \Rightarrow\ \exists(Y)((Y\ != SA)\ \ \&\&\ A(Y,X)\ )$

Axiom 4 involves recognition that it is not enough to set up a security administration group, or even to give each admin area its own security group. It tells a dark secret about access control over critical systems. One that is not obvious to non-technical managers reviewing system maintenance activities, and even less obvious when reviewing a desktops user’s environment. People whose job it is to do data transfer have access to most the data in most systems. People whose job it is to do performance tuning can change most operating system configurations. People whose job it is to schedule batch jobs have access to run most jobs on most systems. Etc, etc. etc.

Suppose that IT Management insists on making the security administration group separate from the rest of the system administration team but does not subscribe to Axiom 4, but denies it as in Axiom 5.

> Axiom 5: It is not true that all systems are controlled to some extent by people whose job function is not security.

Again, the formal logical may be skipped. I include it to emphasize the potential for *reduction ad absurdum*, given the true statements about access levels required by the job descriptions above.

Pseudo Code: It is not the case that, for all X, if X is a system then there exists a Y such that Y is a not the security administrator and Y performs actions that affect the ability to control X.

Formal Logic: $\sim \forall (X) \left( (X == S) \Rightarrow \exists(Y)((Y\ != SA)\ \&\&\ A(Y,X) \right)$

It follows that everyone who can affect management's ability to control systems is a security administrator. There are two ways to interpret this:

- reductio ad absurdum
- recognize that security administration is part of the job function of everyone who touches the machine.

Segregation of duties between the security administration and any system maintenance process would have the result that security administrators have *responsibility* for maintaining access control when they do not have the *power* to maintain that control. That is, administrators who have equal privileges due to the installation and maintenance responsibilities that are part of their own job functions can change any security-related configuration. A logical CIO will take the latter interpretation: that security administration is part of the job function of everyone who touches the machine.

With this interpretation comes the recognition that IT Security is by nature distributed. Where any significant need for IT Management exists, CIO delegation of authority exists, and organizational processes exist. Security controls should align with the processes that run IT.

Therefore, in order for the CISO's rulebook to protect the firm, it cannot just map out what IT Security must do, it must map directly onto the CIO's existing delegated authority structure. Part of the job of the CISO is to identify the place where the policy compliance matters most, and make sure the person in that job function knows that the rulebook applies to them.

The key to effective security is the recognition on the part of CIO that the ability for security to set some rules is not limited to functions that one would traditionally think of as a security function. So let us say a CISO has a wise and logical CIO, and thus has the go-ahead to create a rulebook that will result in secure systems. The scope of the security rule set is the scope of organizational processes that can affect systems.

IT, as one of the major enablers of the business, will have many organizational processes that affect systems. In an efficient organization, all of them will. A CISO should recognize the strength of management commitment to each process. The degree to which the process is universally followed is the degree to which it can be exploited to increase the clarity of a security directive. A CISO can leverage this commitment to process by understanding the key goal indicators and key performance indicators of the process and showing how, by combining security activities into the process critical success factors, and using security metrics as key performance indicators, key goal indicators are more easily realized.

Of course, management processes within Bear are highly proprietary, and I cannot use them as examples here. So instead, I present industry standard management IT control processes (the source is COBIT).

**PLANNING AND ORGANISATION**
**PO1** Define a Strategic IT Plan
**PO2** Define the Information Architecture
**PO3** Determine Technological Direction
**PO4** Define the IT Organisation and Relationships
**PO5** Manage the IT Investment
**PO6** Communicate Management Aims and Direction
**PO7** Manage Human Resources
**PO8** Ensure Compliance with External Requirements
**PO9** Assess Risks
**PO10** Manage Projects
**PO11** Manage Quality
**ACQUISITION AND IMPLEMENTATION**
**AI1** Identify Automated Solutions
**AI2** Acquire and Maintain Application Software
**AI3** Acquire and Maintain Technology
Infrastructure
**AI4** Develop and Maintain Procedures
**AI5** Install and Accredit Systems
**AI6** Manage Changes
**DELIVERY 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** Assist and Advise Customers
**DS9** Manage the Configuration
**DS10** Manage Problems and Incidents
**DS11** Manage Data
**DS12** Manage Facilities
**DS13** Manage Operations
**MONITORING**
**M1** Monitor the Processes
**M2** Assess Internal Control Adequacy
**M3** Obtain Independent Assurance

**M4** Provide for Independent Audit

Assume these are your management processes. Say P05, Manage the IT Investment, is one your management takes seriously (All COBIT references taken from Management Guidelines, Version 3). Its key goal indicators, that is, its expected contributions to the business, are:

- Percent of IT investments meeting or exceeding expected benefits, based on return on investment and user satisfaction
- Actual IT expenses as percent of total organisation expenses vs. target
- Actual IT expenses as a percent of revenues vs. target
- Percent of business owner IT budgets met
- Absence of project delays caused by lags in investment decisions or unavailablity of funding

Its key performance indicators, that is, the process measurements IT uses to manage it, are:

- Percent of projects with business owners
- Months since last review of budgets
- Time lag between deviation occurrence and reporting
- Percent of project files containing investment evaluations
- Number of projects where business benefits are not verified post-facto
- Number of projects revealing investment or resource conflicts after approval
- Number of instances and time-lag in delayed use of new technology

At a glance, P05, Managing the IT Investment, seems to have nothing to do with security. But on a closer look at the goals and performance indicators shows that making security part of the IT investment process can head off potential problems down the line. For example, any plan to meet goals concerning budgets met or project delays can easily be shown to require forethought with respect to security. A CISO should easily be able to come up with examples of incidents to support a rule that security requirements must be part of the project return on investment.

Where a CISO does not have a ready example of a plane crash caused by an unsafe configuration, he or she reaches the boundaries of acceptance. An effective CISO will also be a good story-teller, using facts about technology as premises and potential accidents as conclusions. As long as the premises lead accurately to the theoretical conclusions, security considerations should be considered necessary process components. The acceptance of the possibility of the scenario lays the groundwork for accident prevention.

Here is an example of how security can find a niche in an seemingly non-security related process like Managing the Investment:

- User requests desktop program from dedicated desktop admin
- Admin checks “approved” list, requested program is not there
- Admin advises user to make formal request through software acquisition process

- Software acquisition process requires desktop engineering approval
- Control point within desktop engineering approval is “security review”
- Security Reviews request, bringing admin and/or back for configuration consultation if required

Desktop Administration does not  want to take responsibility for telling a user that they cannot use a much desired, but inherently risky application.  That job is to provide IT service, not to refuse it.  They are happy to announce that, although the “special” service or product exists, they cannot purchase it because it does not comply with IT Security rules.  It is the role of the CISO to defend that decision.

So much the better if the admin taking the special order actually has no way to provision the requested service without IT Security getting wind of it.  This allows the admin to say, “I’d love to help you, but we would just be spinning our wheels because once it hit IT Security, they would stop it anyway.”  At that point, the admin may pick up a conference line to see if there is a way that together, IT Operations and IT Security can figure out how to secure the product or service and make the user happy.  This creates a new rule in the rulebook.

Staff that is dedicated to IT Security should be focused on identifying loopholes in processes that could allow lapses in security, and closing them with an appropriate delegation of responsibility, a monitoring function, or an escalation to Security.  Because security is integrated into the process, the results of security monitoring are immediately understood by all process participants. It is understood that is not the function of IT Security to handle all security related tasks.  Rather, it is the function of IT Security to ensure that operations maintains security.  This includes ensuring that there are appropriate tools and techniques to do so.

Mapping Security onto mature processes provides a cost-effective approach that minimizes the number of people required to be fully utilized as IT Security Staff. Everyone with system administration privileges is responsible for maintaining security. Checkpoints within independent processes provide assurance that IT Security is maintained.

In order for an IT Security group to be successful with this approach, it must meet key goal indicators that the business has for IT Security.  That is, the resulting processes must maintain the confidentiality,integrity, and availability of data.  Performance indicators will vary with the actual process with which security is aligned, but these are some general ones:

- Policy is clear for all platforms and standards are clear for platforms where risk levels are high or distributed administration is prevalent
- Security review and approval is part of the System Software and Architecture Lifecycle, especially with respect to security software selection and configuration, and new network connectivity
- Configuration change control is monitored

- User administration processes are controlled
- Security incidents are investigated

So as long as the resulting rulebook and CISO decision process is focused on the objective of maintaining management control over computers, a CIO will be happy to endorse this process participation. Security's participation in other IT process will lead not only to a more effective security rulebook, but lead to more controlled, thus more effective IT processes overall. The actual rules in the rulebook are nothing a CIO need be bothered with any more than they scrutinize a trusted accountant over the Rules for Spending Authorization. There are competent professionals that are more than capable of authoring them. As long as those who are governed by them understand them and are not overly critical of their contents, the CIO relies on the CISO to work out the details.