MEETING FFIEC REQUIREMENTS WITH CIMTRAK

In the not too distant past, information security programs were an afterthought at many financial institutions. With the passage of the Gramm-Leach-Bliley Act (GLBA) in 1999, institutions were mandated to make information security a key part of their business strategy and planning.

Today, the Federal Financial Institutions Examination Council (FFIEC) provides guidance to financial institutions as it relates to the security of IT assets and information.

COMPREHENSIVE CHANGE DETECTION

Detect all changes to a wide variety of systems including those that are virtual or cloud based.

COMPLETE AUDIT TRAILS

Be able to track changes as they occur and have complete documentation on them.

FORENSIC DETAIL OF CHANGES

Know who is making changes, how they are being made and where they originate from.

CONTINUITY OF OPERATIONS

CimTrak offers the option to instantly restore changes, keeping your critical information accessible.

EXTENSIVE REPORTING

CimTrak provides a wide variety of reports on watched systems as well as internal reporting on CimTrak users.

THE GRAMM-LEACH-BLILEY ACT

The Gramm-Leach-Bliley Act repealed part of the Glass–Steagall Act by removing barriers in the market among banking companies, securities companies and insurance companies that prohibited any one institution from acting as any combination of an investment bank, a commercial bank, and an insurance company. Section 501(b) of the Gramm-Leach-Bliley Act (GLBA) required the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision to establish standards for protecting the security and confidentiality of financial institution customers' non-public personal information. To that end, Section 501(b) subsection 314.3, known as the Safeguards Rule, required institutions to implement an information security plan and achieve the following objectives:

1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Section 501(b) of the Gramm-Leach-Bliley Act required the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision to establish standards for protecting the security and confidentiality of financial institution customers' nonpublic personal information.

THE FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (FFIEC)

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) to make recommendations to promote uniformity in the supervision of financial institutions. To encourage the application of uniform examination principles and standards by the state and federal supervisory authorities, the Council established, in accordance with the requirement of the statute, an advisory State Liaison Committee composed of five representatives of state supervisory agencies. In accordance with the Financial Services Regulatory Relief Act of 2006, a representative state regulator was added as a voting member of the Council in October 2006.

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions to make recommendations to promote uniformity in the supervision of financial institutions.

The FFIEC publishes guidance that helps financial institutions implement information security processes. In 2006, the FFIEC published the IT Examination Information Security Handbook which assists institutions in achieving a range of IT security objectives including Availability, Integrity of Data or Systems, and Confidentiality of Data or Systems. Other IT Examination Handbooks including the Development and Acquisition Handbook, released in 2004, also have sections that address IT security concerns.

HOW CIMTRAK HELPS INSTITUTIONS MEET FFIEC REQUIREMENTS

CimTrak is an integrity and compliance tool that helps financial institutions of all sizes ensure the confidentiality, integrity, and availability of critical IT systems and data. Today's IT networks are not solely comprised of a few servers, but rather a complex web of systems, applications, and devices that must function properly at all times. Based on cutting edge file integrity monitoring, CimTrak allows users to go beyond simply monitoring files for changes to ensuring the overall security of the entire IT environment.

Changes in the IT environment can have devastating consequences be a signal for malicious activity, or a data breach. That's why detecting changes and being able to respond to them quickly is a critical component of a solid IT security program. This is all the more critical for financial institutions that rely heavily on IT systems to interact with customers, process transactions, and store sensitive customer and corporate data. Changes that cause system downtime and data breaches can be extremely costly and cause a loss of customers and reputation, not to mention the time spent trying to rectify the situation.

CimTrak scales to the largest environments, but is also budget friendly to meet the needs of smaller institutions. Offering change detection for a wide range of servers, workstations, network devices, databases and applications including Active Directory and other software packages specific to financial institutions, changes can be monitored from one central tool. CimTrak even detects changes to virtual environments, web applications and infrastructure that may be housed in the cloud.

Offering change detection for a wide range of servers, workstations, network devices, databases and applications including Active Directory and other software packages specific to financial institutions, changes can be monitored from one central tool.

CimTrak

» Detects changes across heterogeneous IT environments of all sizes
» Quickly alerts IT personnel to changes that can have negative consequences
» Pinpoints changes to help quickly identify, resolve problems and mitigate threats
» Creates reports that greatly simplify reporting to management and auditors

CIMTRAK IS SECURITY

CimTrak has been built with the stringent needs of government customers in mind. CimTrak has been certified to Common Criteria EAL Level 4 + FLR, the highest government certification for a software product. In addition, the CimTrak cryptographic module has been certified to meet the Federal Information Processing Standard (FIPS) 140-2. Further, your critical data is secure. All communications between CimTrak components are fully encrypted and the CimTrak Master Repository stores your files and configurations in both a compressed and encrypted form. No other integrity and compliance tool can match these stringent safeguards to protect your information.

With coverage for a wide range of systems, devices, and applications, CimTrak fits in your environment. What's more, CimTrak is easy to set up, configure and use, so your IT staff can spend time on more pressing issues. By providing key insight into your IT environment, personnel can pinpoint issues and react quickly, maximizing time and saving money. It's why enterprises and government agencies worldwide rely on CimTrak to ensure integrity and maintain compliance with regulations such as those dictated by the FFIEC.

REQUIREMENT	HOW CIMTRAK HELPS
FFIEC DEVELOPMENT AND ACQUISITION IT EXAMINATION HANDBOOK (2004) **OBJECTIVE 13: ASSESS THE SECURITY AND INTEGRITY OF SYSTEM AND APPLICATION SOFTWARE.** 1. Assess the quality of open source-code system documentation by evaluating the adequacy of internal and external assessments of: » The adequacy of program change controlsto enforce its authorized change requests and collect unauthorized attempts in the form of intrusions.	CimTrak detects all changes to applications, including those under development. By utilizing CimTrak's Update Baseline mode, incremental changes to code can be tracked and changes rolled back if necessary.
FFIEC INFORMATION SECURITY IT EXAMINATION BOOKLET (2006) **TIER II OBJECTIVES AND PROCEDURES** *Part B: Network Security* 10. Determine whether firewall and routing controls are in place and updated as needs warrant.	Using CimTrak for Network Devices, IT staff can be alerted to any changes to firewall and router configurations ensuring that malicious changes or accidental changes can be quickly investigated and remediated.
Part C: Host Security 8. Determine whether the host-based IDSs identified as necessary in the risk assessment are properly installed and configured, that alerts go to appropriate individuals using an out-of-band communications mechanism, and that alerts are followed up.	The IT security examination booklet specifically discusses the use of integrity checking software such as CimTrak (sometimes referred to as a host-based IDS or HIDS) in order to detect all changes to hosts. The goal is to detect malicious changes such as root kits, logic bombs, or even malware that may evade traditional anti-virus tools. CimTrak detects and alerts IT personnel to all changes on hosts which allows timely alerting, investigation, and remediation of threats to the security of the IT environment.
Part M: Security Monitoring 5. Determine whether logs of security-related events are sufficient to support security incident detection and response activities, and that logs of application, host, and network activity can be readily correlated.	CimTrak generates complete audit trails of all detected changes, which allows for simple investigation of events as well as reporting for both management and auditors.
FFIEC CLOUD COMPUTING GUIDANCE (2012) **INFORMATION SECURITY** "Storage of data in the cloud could increase the frequency and complexity of security incidents. Therefore, management processes of financial institutions should include effective monitoring of security related threats, incidents, and events on both financial institutions' and servicers' networks; comprehensive incident response methodologies; and maintenance of appropriate forensic strategies for investigation and evidence collection."	With cloud computing gradually becoming more prevalent in many organizations including those in the financial space, the need for securing data and applications in the cloud is becoming ever more crucial. While many security tools do not work well or at all in a cloud environment, CimTrak works equally well in a physical, virtual or cloud environment, detecting changes that can compromise valuable systems or data.