



White paper

STAYING COMPLIANT WITH THE EVOLVING SECURITY REGULATIONS OF GLBA

Prepared by:

Paul Reymann
President
ReymannGroup, Inc.

Mitchell Ashley
VP of Engineering & CIO
Latis Networks, Inc.

May 2003

Table of Contents

Introduction	3
Purpose of the new guidance	3
Affected organizations	3
Penalties for noncompliance	3
Summary of the new FFIEC guidance	3
Component 1: Information security risk assessment	3
Component 2: Security strategy development	4
Component 3: The implementation of security controls	4
Component 4: Security testing	5
Component 5: Continual monitoring and updating of the security program	5
Tools to promote compliance	5
StillSecure Border Guard	5
StillSecure VAM	6
Conclusion	7
Additional information and guidance	7
Appendix A. Network security self-assessment checklist	8

About the author

Paul Reymann is one of the nation's leading financial industry regulatory experts and co-author of Section 501 of the Gramm-Leach-Bliley Act (GLBA). Mr. Reymann has more than 18 years of experience in the financial services industry, including 13 years with the Department of Treasury's Office of Thrift Supervision (OTS) in Washington D.C. There, he guided the regulatory agency's Technology Risk management activities and authored several key regulatory directives and advisories on emerging risk management issues, including the industry's first regulatory directive on transactional Internet banking.

Mitchell Ashley, as Vice President of Engineering & CIO of Latis Networks, Inc., is responsible for the product strategy and development of the StillSecure™ suite of network security software. Mr. Ashley brings to Latis Networks more than 20 years of experience in data networking, network security, and software development. Mr. Ashley is a graduate of the University of Nebraska, with a Bachelor of Science degree in Computer Science and Business

1. INTRODUCTION

In January 2003 the member agencies¹ of the Federal Financial Institutions Examination Council (FFIEC) issued new examination guidance that expands on the GLBA Data Protection Rule. The new guidance requires banks to take specific action to protect all information assets, not just customer information.² The guidance is specified in the FFIEC Information Security IT Examination Handbook, published in December 2002.

This paper provides a high-level summary of the new guidance and describes network security tools that can help you comply with the updated regulations.

Purpose of the new guidance

The new FFIEC guidance provides detailed instructions for deploying a continuous holistic information security program. Affected financial institutions must implement an information security program that integrates people, processes, and technology to:

- **Identify and manage risks**
- **Test risk management practices**
- **Monitor the information security environment to control risks continuously, not point-in-time.**

In clarifying the philosophy behind the new guidance, the FFIEC states: "Security is an ongoing process, whereby the condition of a financial institution's controls is just one indicator of its overall security posture. Other indicators include the ability of the institution to continually assess its posture and react appropriately in the face of rapidly changing threats, technologies, and business conditions."

The FFIEC member agencies defined such a process-based approach to security in the GLBA Data Protection Rule. This new examination guide espouses the same process-based approach, applies it to various aspects of the financial institution's operations, and serves as a supplement to the banking agencies' GLBA Data Protection expectations.

Affected organizations

The FFIEC's GLBA Data Protection Rule and these supplemental examination guidelines apply to all federally insured depository financial institutions. The guidelines give the FFIEC agencies the power to enforce compliance and take action if financial institutions do not establish and maintain adequate information security programs.

¹ FFIEC member agencies include 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 Office of Thrift Supervision (OTS).

² GLBA Data Protection rule that took effect on July 1, 2001 applied to protecting non-public person customer information only, not other data such as an institution's corporate or commercial customer information. For additional information on the GLBA Data Protection Rule, refer to Latis Networks' September 2002 White Paper – "The Data Protection Rule of the GLBA - A strategy for compliance."

Penalties for noncompliance

Institutions found to be noncompliant with the rules or that have deficiencies in their administrative, technical, or physical safeguards are subject to regulatory enforcement measures ranging from corrective action to fines or other penalties.

Regulators have not shied away from assessing penalties on GLBA violators. On April 7, 2003, the Office of the Comptroller of the Currency (OCC) – an FFIEC member agency – announced civil monetary penalties against two bank employees who violated the GLBA rules. "National bank customers have a right to expect that the confidentiality of their financial information will be protected," said Comptroller of the Currency John D. Hawke, Jr. "The OCC will respond aggressively if we find that bank employees are misusing information, or placing it at risk of unauthorized disclosure."

2. SUMMARY OF THE NEW FFIEC GUIDANCE

The new FFIEC guidance encourages financial institutions to implement an information security process that includes the following five components:

1. **Risk assessment**
2. **Security strategy development**
3. **Implementation of security controls**
4. **Security testing**
5. **Continual monitoring and updating of the security process**

The following subsections summarize the FFIEC expectations with respect to each of these components.

Component 1: Information security risk assessment

A risk assessment is a pre-requisite to forming the strategy that guides the institution in developing, implementing, testing, and maintaining its information security culture. The initial risk assessment may involve a significant one-time effort, but the risk assessment process should be an ongoing part of the security program.

The guidance recommends a three-phased approach for conducting the risk assessment:

1. **Gather data** on key assets, threats to such assets from malicious or non-malicious people and events, organizational and technical vulnerabilities, and existing controls. This phase should include a device-by-device inventory of information system assets and a vulnerability assessment to identify weaknesses on hardware, software, networks, workstations, and remote access devices.
2. **Analyze the data** gathered in phase 1 to characterize the system, identify and measure threats to the system, and estimate the probability of known and unknown threats taking action against the system. Comprehensive threat scenarios³ should be used to gain insight into the impact and importance of identified threats.
3. **Prioritize the risks** identified during the analysis phase and develop an appropriate mitigation strategy.

Component 2: Security strategy development

The guidance suggests defining a Board-approved security strategy specifying control objectives and establishing an implementation plan. GLBA, Sarbanes-Oxley, and now the new FFIEC guidance all emphasize the importance of the Board's involvement in the organization's risk management and information security programs. The emphasis on Board participation underscores the shift in the perceived importance of security issues: no longer only the concern of the IT department, data security and control have become a high-level business priority.

The security strategy should promote:

- Layered controls that establish multiple control points between threats and key assets
- Policies that guide personnel in implementing the security process
- Cost comparisons of different strategic approaches appropriate to an institution's environment and complexity, normalized to the size of the organization.

An effective information security strategy is essentially a plan to mitigate risk and comply with mandated laws, rules, contractual requirements, and internal policies. The foundation for an effective strategy includes:

- Defining control objectives
- Identifying and assessing ways to meet objectives
- Selecting controls
- Establishing benchmarks and metrics to measure and maintain the controls
- Defining a formal test plan to validate the effectiveness of the control environment.

Think of a control as an approach for mitigating a specific identified risk. For example, a control could be a network intrusion-detection policy. Such a policy might consist of simply reviewing the daily access logs. Alternatively, it could entail installing network and host-based intrusion-detection systems. Each organization needs to identify and justify the appropriate controls based on the identified risks. In this example, the first option (i.e., access log review) might be perfectly appropriate for protecting the integrity of an information-only Web site. The second, more elaborate option (host and network IDS) would be the appropriate control for an organization maintaining a sophisticated Internet banking capability.

³ An example of a general malicious threat scenario is an unskilled attacker using a program script to exploit a vulnerable Internet-accessible Web server to extract sensitive information from the institution's database. In such a scenario, where identity theft is a probable result, customers are likely to be the ultimate victims.

Policies and their consistent application and enforcement are at the heart of a successful security strategy. Effective policies are communicated to staff, are flexible to address environmental changes, and are regularly reviewed and updated.

Component 3: The implementation of security controls

The FFIEC guidance provides an in-depth overview of the various administrative, physical, and technical controls that must be considered when protecting financial data. The guidance describes and specifies the performance expectations for controls in the following areas:

- Logical and administrative access control
- Physical security
- Encryption
- Malicious code controls
- Systems development, acquisition, and maintenance
- Personnel security
- Electronic and paper-based media handling
- Logging and data collection
- Service provider oversight
- Intrusion detection and response
- Insurance.

The following paragraphs highlight just a few of these controls and FFIEC's expectations for how they should be implemented and maintained.

Within the category of *Logical and administrative access controls*, the guidance discusses the technologies that govern network access, including protocols and ports, routing, TCP/IP packets, and network configuration. In this context, the guidance describes the use and management of network firewalls.

Incoming and outgoing traffic between security domains must pass through a firewall. Firewalls are ideally situated to inspect and block traffic, coordinating activities with intrusion detection systems. Firewalls analyze and block unauthorized traffic using one of four primary techniques: packet filtering, stateful inspection, proxy servers, and application-level types. Each technique has strengths and weaknesses, and financial institutions must analyze the nature of their network traffic to determine the technique that fits best within their network environment.

The guidance makes it clear that firewalls alone are not sufficient to secure a network: "Firewalls should not be relied upon, however, to provide full protection from attacks. Institutions should complement firewalls with strong security policies and a range of other controls. In fact, firewalls are potentially vulnerable to attacks" including spoofing, denial-of-service, sniffing, hostile code embedded in legitimate traffic, the exploitation of unpatched vulnerabilities.

The guidance discusses intrusion detection as an option for defending against the attacks that get through the firewall. Effective intrusion detection is a two-stage process: detecting intrusions in stage one,

and properly responding to them in stage two. The guidance states “The earlier an intrusion is detected, the greater the institution’s ability to mitigate the risk posed by the intrusion. Financial institutions should have a capability to detect and react to an intrusion into their information systems.”

Component 4. Security testing

The testing mandated by the FFIEC guidance is designed to verify that the implemented security controls are effective. Typical testing only measures security posture at a specific point-in-time. Security testing should be conducted frequently to ensure that your information security controls are working effectively over time.

Testing should be commensurate with the institution’s risk profile: high-risk systems should be tested more frequently than low-risk systems. In general, risk increases as additional access is granted to sensitive data and processes.

Management may decide to perform a range of tests to completely validate security effectiveness. For example, “independent diagnostic tests” include penetration tests, audits, and assessments. Independence is key – it provides credibility to the test results.

System vulnerability assessments are an important element of a testing program. These assessments locate security vulnerabilities on systems, such as one or more hosts and networks, and identify corrective actions. The guidance recommends that “network vulnerability scanning can occur at least as frequently as significant changes are made to the network.” In even moderately complex networks, such changes occur daily or even hourly. Accountability is also emphasized: “Test results that indicate an unacceptable risk in an institution’s security should be traceable to actions subsequently taken to reduce the risk to an acceptable level.”

Component 5. Continual monitoring and updating of the security program

The monitoring and updating component consists of gathering and analyzing data on new threats and vulnerabilities, actual attacks, and the effectiveness of your security controls.

Cycling this data back into the risk assessment strategy and controls creates a continuous and dynamic information security program. A static program creates a false sense of security and is ineffective over time. Monitoring and updating the security program is a critical requirement for effective security. The authors of the guidance state that “management and security personnel must remain alert to emerging threats and vulnerabilities,” and they single-out automated tools as a particularly effective element of a monitoring program. “Security personnel should have access to automated tools appropriate for the complexity of the financial institution systems. Automated security policy and security-log analysis tools can significantly increase the effectiveness and productivity of security personnel.”

TOOLS TO PROMOTE COMPLIANCE

In an effort to help financial institutions assess network security practices and evaluate their compliance readiness, The Reymann Group and Latis Networks have created a self-assessment checklist,

presented in Appendix A. In addition to serving as a quick-reference for gauging your security preparedness, the checklist indicates areas where the Latis Networks’ StillSecure line of security software can play an instrumental role in securing the network and complying with the updated guidance.

The StillSecure suite of network security products includes:

- **Border Guard** – a family of intrusion prevention products that automatically block network attacks.
- **VAM** – a Vulnerability Assessment and Management tool that identifies vulnerabilities on the network and tracks remediation activities through to a verified repair.

StillSecure products, discussed in more detail below, provide a wide range of benefits including:

- Helping organizations set and ensure security policy
- Testing network components from internal or external views
- Providing reports and historical data for compliance reporting.

StillSecure products are uniquely capable of assisting the financial services industry comply with GLBA and this enhanced regulatory guidance. Collectively these products provide a number of the security controls for both the (1) attack prevention and (2) assessment and testing that the new guidance specifies. They also include reporting and accountability features designed for auditors, regulators, and high-level management oversight. The suite of software forms the backbone of a comprehensive information security program.

StillSecure Border Guard

Protects you from the cost of malicious intrusions

Border Guard products reduce the risk and liability from network attacks by terminating malicious network traffic. Employing our exclusive *Dynamic Attack Detection*[™] and *Dynamic Attack Response*[™] technologies, Border Guard products identify and terminate the attacks and harmful traffic that would damage your network. The Border Guard family consists of three products that collectively protect a variety of network architectures:

- **Border Guard Standard** – works in concert with your existing firewall to block attacks.
- **Border Guard Gateway** – blocks malicious attacks in real-time, independent of firewall functionality.
- **Border Guard Wireless** – prevents intruders from compromising your network through notoriously insecure wireless access points.

Figure 1 shows where these products could be installed on the network. Border Guard products respond to anomalous behavior that matches a continuously updated directory of rules. Through *Intelligent Attack Profiling*[™], each Border Guard installation characterizes the traffic moving across the network and learns how to best respond to anomalous patterns by terminating the traffic, sending alerts, or allowing access.

StillSecure VAM

Eradicates Vulnerabilities through continuous Assessment and Management

The VAM family of Vulnerability Assessment and Management products identifies, tracks, and manages the repair of vulnerabilities on your network that could leave you exposed to attack. The vulnerabilities found during network scans are tracked through VAM's exclusive *Vulnerability Repair Workflow™*, which manages the remediation process through to a verified repair. VAM produces a range of detailed reports customizable for auditors, managers, and IT staff.

The VAM family includes three products that collectively secure all network devices:

- **Server VAM** – scans servers, routers, switches, and other network infrastructure devices located behind your firewall.
- **Desktop VAM** – optimized for desktops, laptops, and printers.
- **Remote VAM** – scans Internet-visible devices in the network perimeter.

VAM family products (see Figure 2) integrate seamlessly. All products can be installed on a single server and managed through a single user interface. The scan results, reports, and repair tasks generated by VAM products can be rolled up into a single display or viewed individually by product, giving enterprises of all sizes the flexibility needed to efficiently eliminate potentially catastrophic network vulnerabilities.

Conclusion

The updated guidance specified by the FFIEC is complex and comprehensive. It addresses virtually every system or process that influences information security, from access policies to the proper management and oversight of IT service providers. StillSecure network security products are ideally suited for organizations required to comply with GLBA and the updated guidance. The StillSecure suite establishes a solid foundation on which to build an effective security strategy and provides the features financial institutions need to meet reporting, accountability, and traceability requirements.

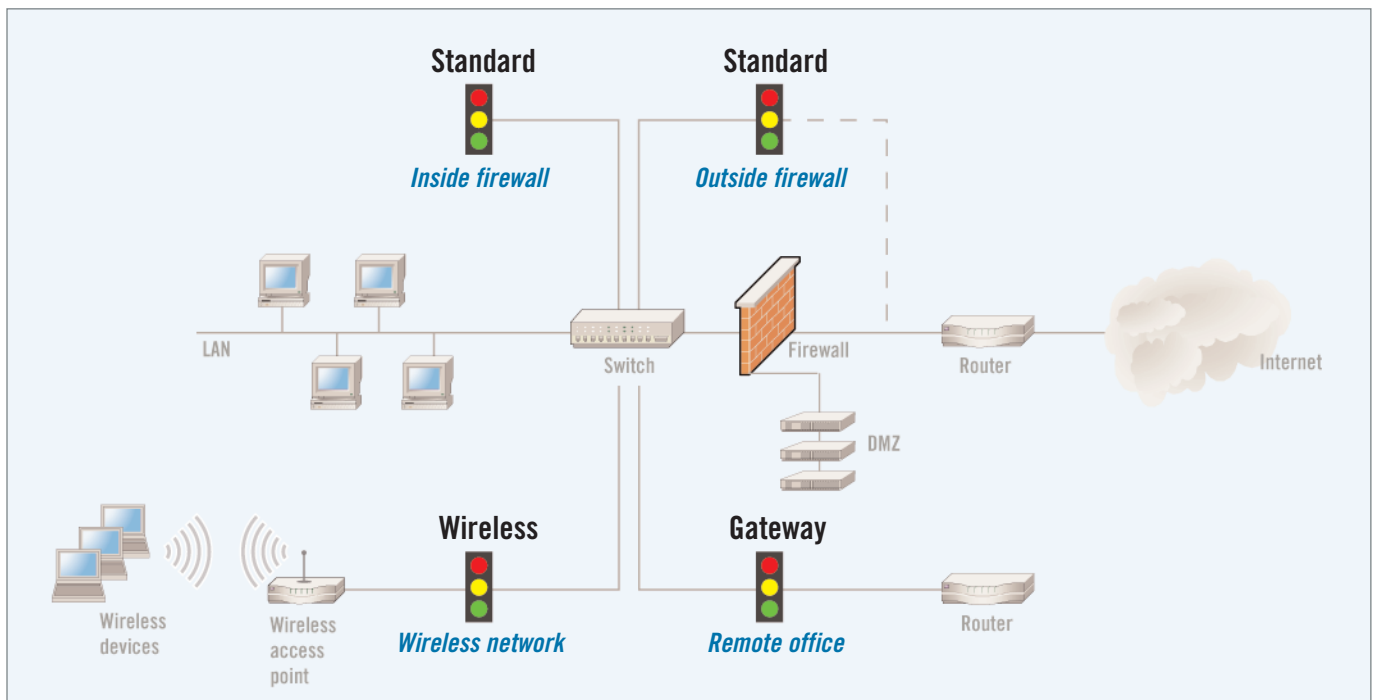


Figure 1. Typical Border Guard product installations.

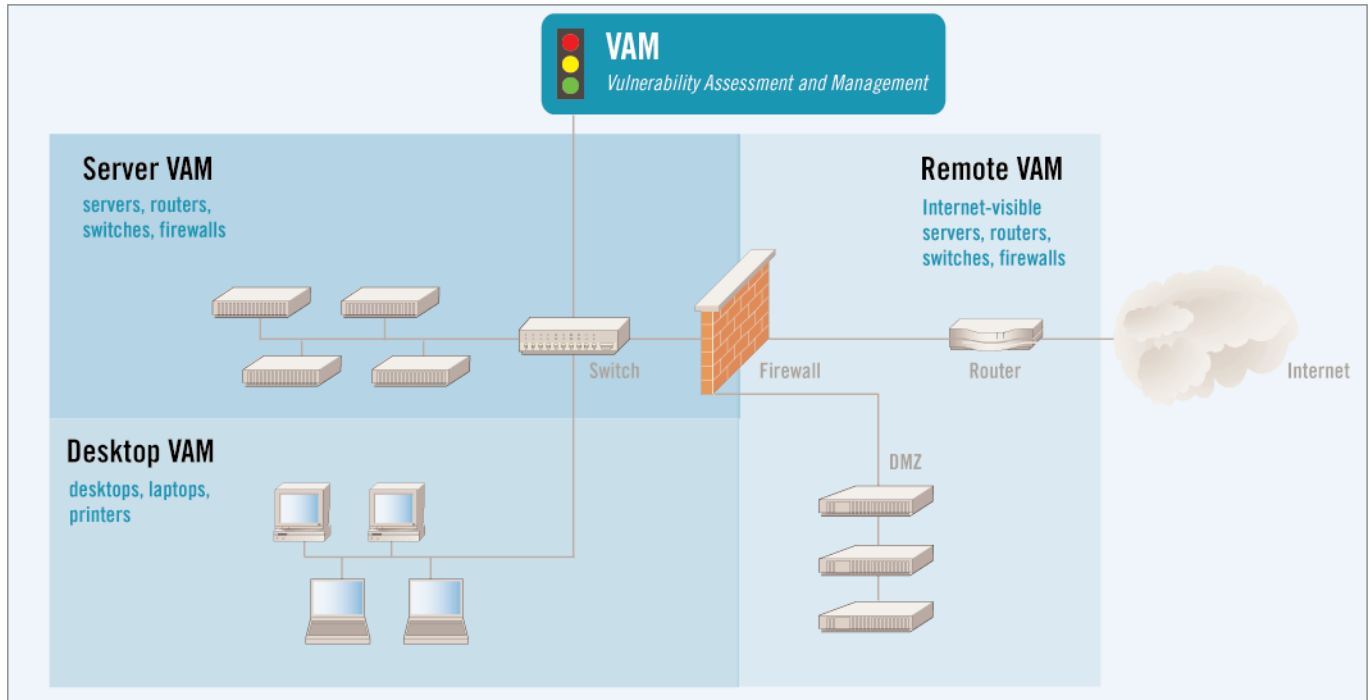


Figure 2. A typical StillSecure VAM installation. All three VAM products can be installed on a single machine and managed from one user interface. The shading indicates the coverage each VAM product provides.

ABOUT LATIS NETWORKS

Latis Networks provides affordable, easy-to-use network security software products for IT and security professionals at security-conscious mid-tier enterprises. The StillSecure suite reduces the risk and liability of damages from network attacks and tangibly increases the productivity and effectiveness of your resources. StillSecure is available through Latis Networks' direct sales force and channel partners. Latis Networks is financed by Mobius Venture Capital, 3i, and Feld Group Ventures. For more information please call (303) 381-3830, or visit our website at www.stillsecure.com.

ABOUT REYMANN GROUP, INC.

ReymannGroup assists financial institutions in assessing risks and determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with key regulatory requirements. Through our formal program review and gap assessment service, we provide you with "independent" high-caliber professionals and knowledge experts that help you achieve GLBA Data Protection and USA Patriot Act compliance. We have authored several banking regulations and are experts familiar with banking industry regulations and best practices. Our services will meet and exceed your business need to implement and maintain safe, sound, and secure compliant programs. Visit www.reymanngroup.com to learn more or contact Paul Reymann at (410) 867-1564 or paul@reymann.name.

ADDITIONAL INFORMATION AND GUIDANCE

Additional information and guidance about how to develop a compliant information security program is available from the following Internet URLs.

- **December 2002 FFIEC Information Security Guidance Booklet:** You can obtain a copy of the new examination guidelines at: http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf
- **Final GLBA Rule:** You can obtain a copy of the final regulations by visiting the following Regulatory agency sites:
 - Federal Banking Agencies:** <http://www.occ.treas.gov/fr/fedregister/66fr8616.htm>
 - FTC:** <http://www.ftc.gov/os/2000/05/65fr33645.pdf>
 - SEC:** http://www.sec.gov/rules/final/34-42974.htm#P454_179663
- **Whitepaper: The Data Protection Rule of GLBA – a strategy for compliance.** The Reymann Group and Latis Networks have written this summary whitepaper for financial services organizations. http://www2.stillsecure.com/index.jsp?sector=papers_briefs.

APPENDIX A: NETWORK SECURITY SELF-ASSESSMENT CHECKLIST

<i>Self-assessment questions</i>	<i>StillSecure™ capabilities</i>	<i>Your readiness</i>
1. Do you monitor your enterprise's security infrastructure in real-time?		<input type="checkbox"/>
2. Do you analyze and correlate network security events across a variety of devices?		<input type="checkbox"/>
3. Do you use a combination of network and host intrusion detection sensors?		<input type="checkbox"/>
4. Do you gather data on:		
• Key assets?		<input type="checkbox"/>
• Threats to key assets from malicious or non-malicious people and events?		<input type="checkbox"/>
• Threats to key assets from organizational and technical vulnerabilities?		<input type="checkbox"/>
• Effectiveness of existing controls?		<input type="checkbox"/>
5. Do you analyze the probability and impact associated with known threats and vulnerabilities to key assets?		<input type="checkbox"/>
6. Does your network security address:		
• Monitoring of inbound and outbound Internet traffic?		<input type="checkbox"/>
• Filtering malicious code?		<input type="checkbox"/>
• Coordinating with intrusion detection and response mechanisms?		<input type="checkbox"/>
• Operational anomalies that may act as intrusion-warning indicators?		<input type="checkbox"/>
7. Do you perform independent diagnostic tests?		<input type="checkbox"/>
8. Do your security monitoring activities include:		
• Reviewing security and activity events and logs?		<input type="checkbox"/>
• Investigating operational anomalies?		<input type="checkbox"/>
• Routinely reviewing system and application access levels?		<input type="checkbox"/>
• Use of automated security analysis tools?		<input type="checkbox"/>
9. Do you provide management with reports that help them make informed security decisions?		<input type="checkbox"/>
10. Are your reporting capabilities consistent with the GLBA Data Protection rules?		<input type="checkbox"/>