

BASIC FTC RED FLAGS CHECKLIST

by JJ Thompson

6-August-09

Element:

Identify what red flags could occur in your environment

authorities, and assessment of the impact on your organization

Overview of Requirement:

This procedure should outline a means to identify red flags and what occurrences may be considered a red flag. In particular, this includes:

- A complaint or question from a customer based on their receipt of another's bill; a bill for a product or service that recipient denies receiving; a bill from an entity that the customer never patronized; an EOB from a provider for services that were not received
- Records showing treatment or services that are inconsistent with history as reported by customer
- A complaint or question from a customer about the receipt of a collection notice from a bill collector
- A customer, patient, or insurer report that stating that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a cap has been reached

Element:

Indicate how you will **detect** red flags

Overview of Requirement:

This procedure should identify your process to:

- Train staff on identity theft and red flags detection
- Assign a staff member to investigate possible red flags
- Institute measures to detect red flags, such as identity verification and authentication, address change confirmation and provide customers with information about how to be more aware about identity theft risks

Element:

Establish a procedure for responding to red flags

Overview of Requirement:

This procedure will identify your process to:

- Plan for gathering documentation if an incident occurs
- Process for reporting and the contact to whom to report an incident
- Guidelines for appropriate action, such as cancelling the transaction, notification of the customer and or

Element:

Review & update your red flags program at least annually

Overview of Requirement:

You should continually review and update your procedures and policies as applicable, based on your organization's experience and any changes based on a risk assessment.

Element:

Incorporate specific **administrative elements** into your red flags program.

Overview of Requirement:

Incorporate the specified administrative elements into your red flags program:

- Board of directors, appropriate committee or managing partner approval of the written policies and procedures
- A specified staff member assigned to oversee implementation of policies & procedures
- All staff receiving training on the policy and procedures
- The policy and procedures are applied to arrangements with your service providers, and you receive evidence annually to support their compliance

How We Help Companies Succeed

Rook provides IT Risk Advisory services that support log management initiatives for organizations at various phases of maturity in their overall monitoring program. Whether your organization is dealing with an emerging regulatory compliance effort, or if you are looking to improve upon your existing program, Rook can provide the methodology and team members with the technical, audit, and management strategy expertise required for success.

Readiness Review - We assess the current state of controls to the desired state of controls to support management strategy, sales enablement, or general compliance efforts. Whether for HIPAA, HITECH, ISO 27002, SOX, PCI, GLBA, FISMA, NIST, or a myriad of other regulations and standards, we provide the knowledge and experience necessary to identify the approach best fit to your organization and prioritized to guide compliance efforts.

Requirement Definition - Working closely with your management and technical teams, we provide experienced professionals who identify the business and technical requirements necessary to a successful log management initiative.

Data Mapping - Whether the scope is known or unknown, we work closely with process owners, system owners, and data owners to determine the data flows for critical and sensitive data, then identify the infrastructure that is in scope

based on the data location when at rest, in use, or as it traverses the network.

Control Identification - When the data mapping is complete and in-scope infrastructure has been identified, controls are identified throughout the process. Identified controls are compared to the desired future state in a gap analysis, and then gaps are documented, and prioritized based on the requirements, budgetary constraints, existing technology, and human factors such as knowledge and internal politics.

Vendor Selection - Requirements are utilized to create Engineering Requirements and a resultant vendor selection matrix. Vendors are reviewed to determine adequacy based on analyst guidance, past experience, internal contacts, and marketing materials. Vendor capabilities are documented, analyzed, the proposal process managed through vendor selection, contract evaluation, and project plan creation.

Health Check - The existing implementation is reviewed to determine if the end-to-end process, team members, and technology (comprising of the Monitoring Program) is operating at optimal efficiency. Areas for improvement are identified, technical configurations are updated, process improvements are managed, documentation updated, and training conducted.