ACH Risk Assessment Standards Manual

September 30, 2019
Version 1.0

OVERVIEW

The **Xtend ACH Risk Assessment Standards Manual** is a designed to assist Xtend in completing a step-by-step ACH Risk Assessment. Xtend is required to perform a risk assessment of their ACH activities and implement a risk management program in accordance with the requirements applicable regulations. Financial institutions are subject to scrutiny regarding both their own ACH operations and those of their third party vendors.

The estimation of risk is based on industry best practice, financial institution examinational manuals, and current risk trends in the industry. Executive management and the board of directors generally fulfill their duties under the business judgment rule by being aware of risk within Xtend and setting the general risk tolerance of the organization. Xtend is not an ACH Originator. Residual risk is partially mitigated through insurance.

RISK DEFINED

Risk of loss is normal and expected within the parameters of business operations. Therefore, the purpose of risk management is to align the risk exposure with the risk tolerance of the organization. When risk is identified, there are four major categories of response:

Avoidance. Do not otherwise engage in the business practice, so risk of loss is no longer a factor. Avoidance strategy is usually employed when potential net losses vastly outweigh potential gains.

Mitigation. Reducing the severity of risk through the institution of controls. Through mitigation, the purpose is to reduce the probability or severity of loss, or both.

Transfer. Requiring that another entity is responsible for remunerating losses. Risk transfer is usually accomplished through insurance.

Acceptance. Acknowledge the risk of doing business and appropriately budget for the potential loss. Accepting high levels of risk within the organization is a normal and sound business practice especially when the cost of reducing risk is substantially greater than the return on investment, and the potential net benefit is substantial.

Executive management and the board of directors generally fulfill their duties under the business judgment rule by being aware of risk within Xtend and setting the general risk tolerance of the organization.

RISK METHODOLOGY

Risk is established through the Factor Analysis of Information Risk (FAIR) method. For each inherent risk, a nine-step process is used to determine residual or remaining risk.

PURPOSE: The purpose of any risk assessment should be the alignment of the organization's risk exposure to the organization's risk tolerance. Risk is defined for the purposes of this report as the probable frequency and probable magnitude of future loss. The management of these risks will be unique to each organization and will change over time.

DISCLAIMER: Risk is always a probability issue. Probability is the continuum between absolute certainty and impossibility. Establishing probabilities is not the same as foretelling the future. Completing this worksheet does not guarantee desirable or undesirable outcomes for the organization. Rather, it allows management to review and determine acceptable levels of risk for the organization.

Step 1. Identify the risk questions and threats.

Step 2. Estimate the probable frequency of the threats. This is a "how often" estimation: how often will the system come under attack, how often will users need to be trained, etc.

Threat Frequency		
Score	**Rating**	**Baseline**
5	Very High (VH)	> 100 times per year
4	High (H)	Between 10 and 100 times per year
3	Moderate (M)	Between 1 and 10 times per year
2	Low (L)	Between .1 and 1 times per year
1	Very Low (VL)	< .1 times per year (once every ten years)

Step 3. Estimate the probable capability of the threats. This is a "how much" estimation: how much skill would it take to infiltrate a system, how much is the project dependent on a vendor, etc. If 98% of the population can figure out how to mount an attack, the threat capability is very high. The easier it is for the threat to impact the project, the greater the capability.

Threat Capability		
Score	**Rating**	**Baseline**
5	Very High (VH)	The threat can easily disrupt the organization.
4	High (H)	The threat will likely disrupt the organization
3	Moderate (M)	There is an even chance the threat will disrupt the organization.
2	Low (L)	The threat is unlikely to disrupt the organization.
1	Very Low (VL)	The threat is very unlikely to disrupt the organization.

Step 4. Record controls. What controls does the organization have in place to resist threats? Recording controls provides assurance that due diligence was taken when developing the project. Controls may include financial and public audit reports of vendors, the sponsorship of the project, etc.

Step 5. Estimate aggregate control strength. This is the ability of identified controls to defeat the capability of the threats.

Aggregate Control Strength		
Score	**Rating**	**Baseline**
5	Very High (VH)	Protects against all but the top 10% of threats.
4	High (H)	Protects against all but the top 70% threats.
3	Moderate (M)	Protects against average (50%) and skill and resources.
2	Low (L)	Protects against only the bottom 30% threats.
1	Very Low (VL)	Protects against only the bottom 10% threats.

Step 6. Derive vulnerability. This is derived by plotting the threat capability against the control strength.

		Vulnerability				
Threat Capability	5 - VH	5 - VH	5 - VH	5 - VH	4 - H	3 - M
	4 - H	5 - VH	5 - VH	4 - H	3 - M	2 - L
	3- M	5 - VH	4 - H	3 - M	2 - L	1 - VL
	2 - L	4 - H	3 - M	2 - L	1 - VL	1 - VL
	1 - VL	3 - M	2 - L	1 - VL	1 - VL	1 - VL
		1 - VL	2 - L	3- M	4 - H	5 - VH
		Control Strength				

Step 7. Derive loss frequency. This is derived by comparing the threat frequency with the vulnerability.

		Loss Frequency				
Threat Frequency	5 - VH	3 - M	4 - H	5 - VH	5 - VH	5 - VH
	4 - H	2 - L	3 - M	4 - H	4 - H	4 - H
	3- M	1 - VL	2 - L	3 - M	3 - M	3 - M
	2 - L	1 - VL	1 - VL	2 - L	2 - L	2 - L
	1 - VL	1 - VL	1 - VL	1 - VL	1 - VL	1 - VL
		1 - VL	2 - L	3- M	4 - H	5 - VH
		Vulnerability				

Step 8. Estimate probable loss. What is the probable financial loss that could occur as a result of the threat? Factors to consider are productivity, response costs, replacement costs, fines and judgments, loss of competitive advantage, and loss of reputation. The chart below is a guideline for assigning loss estimation.

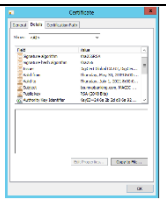
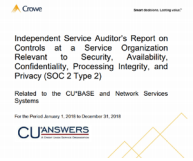
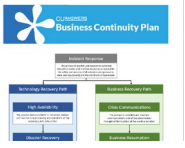
Loss Estimation			
Score	**Magnitude**	**Range Low End**	**Range High End**
5	Very High (VH)	$100,000	
4	High (H)	$50,000	$99,999
3	Moderate (M)	$10,000	$49,999
2	Low (L)	$1,000	$9,999
1	Very Low (VL)	$0	$999

Step 9. Derive risk. This is derived by comparing the loss frequency against the loss magnitude. Whenever possible, risk assessments should be based on whatever hard data is available, but many decisions about the nature of the risk will be based on subjective criteria. To reiterate, the purpose is to give decision-makes the opportunity to estimate the organization's risk exposure and compare that to the organization's risk tolerance.

	Risk					
Loss Magnitude	5 - VH	3 - M	4 - H	5 - VH	5 - VH	5 - VH
	4 - H	2 - L	3 - M	4 - H	4 - H	4 - H
	3- M	1 - VL	2 - L	3 - M	3 - M	3 - M
	2 - L	1 - VL	1 - VL	2 - L	2 - L	2 - L
	1 - VL	1 - VL	1 - VL	1 - VL	1 - VL	1 - VL
		1 - VL	2 - L	3- M	4 - H	5 - VH
	Loss Frequency					

MATERIALS

The following materials are to be reviewed prior to completing the ACH Risk Assessment.

DOCUMENT	PURPOSE	LOCATION/PROVIDER	EXAMPLE
ACH Processing Policy	*Review to ensure policies are current and meet NACHA guidelines for Xtend's ACH activity*	Xtend Bookkeeping Team	
Previous ACH Audit	*Review to ensure all findings have been remediated* *--- OR ---* *Management has agreed to accept the risk*	Xtend Executive Team	
Current Encryption Standards	*Review to ensure encryption remains at an industry-standard or higher level*	CU*Answers Online Banking Team	
CU*Answers SSAE-18 (or similar Reports)	*Review for any significant security exceptions requiring compensating controls by Xtend*	CU*Answers Due Diligence Website	
Xtend Audit Reports	*Review to ensure access to ACH data is audited and maintained*	Xtend Bookkeeping Team	
CU*Answers DR/BR Reports	*Review to ensure FedLine access is tested*	CU*Answers DR/BR Team	

RISK ASSESSMENT WORKSHEETS

1 - VL: Very Low	2 - L: Low	3 - M: Moderate	4 - H: High	5 - VH: Very High

LIFE CYCLE STAGE	DATA IN TRANSIT TO AND FROM THE FEDERAL RESERVE		DATA AT REST			
RISK QUESTIONS	How vulnerable is ACH data to unauthorized exposure in transit?	How likely are communications between CU(BASE and the Fed Reserve to be down?	What is the risk of malicious hacks into our network?	What are the risks of malicious actions by employees?	What is the risk of unauthorized access to ACH information?	What is the risk of data being exposed to the public?
THREATS	External Security	BR/DR	External Security	Employee Risk	Unauthorized Access	Data Exposure
FREQUENCY QUESTION	How frequently will ACH data come under attack?	How frequently will communications be down between CU*BASE and the Fed Reserve?	How frequently will ACH data come under attack?	How frequently will ACH data be missed by employees?	How frequently will ACH data be accessed by unauthorized individuals?	How frequently will ACH data be exposed to the public?
THREAT FREQUENCY	3 - M: Moderate	1 – VL: Very Low	3 - M: Moderate	3 - M: Moderate	3 - M: Moderate	3 - M: Moderate
CAPABILITY QUESTION	How likely will an external attack on ACH data in transit succeed?	How disruptive are these failed communications likely to be?	How likely will an external attack on ACH data in transit succeed?	How likely will employees maliciously use ACH data?	How likely will unauthorized access to ACH data occur?	How likely will ACH data be exposed to the public?
THREAT CAPABILITY	1 - VL: Very Low	4 – H: High	1 - VL: Very Low	1 - VL: Very Low	1 - VL: Very Low	1 - VL: Very Low
IDENTIFIED CONTROLS	System will not function without encryption.	Tested annually through the CU*Answers DR/BR with gap analysis available to Xtend If CU*BASE is unavailable, Xtend will prepare for missing deadlines and what that impact would be on the credit union Xtend would submit share draft returns manually through the credit unions share draft vendor website if needed	Xtend's networks and data hosting is managed by CU*Answers and those controls are described in CU*Answers' annual SSAE-18 reports	Complete background checks for new hires along with strong system security policies	Library software allows financial institutions to control who can see and access reports Xtend performs quarterly access audits	Policies with audit functionality relating to sensitive data left in the public eye
CONTROL STRENGTH	5 - VH: Very High	3 – M: Moderate	5 - VH: Very High	5 - VH: Very High	5 - VH: Very High	5 - VH: Very High
VULNRABILITY	1 - VL: Very Low	4 – H: High	1 - VL: Very Low	1 - VL: Very Low	1 - VL: Very Low	1 - VL: Very Low
LOSS FREQUENCY	1 - VL: Very Low	1 - VL: Very Low	1 - VL: Very Low	1 - VL: Very Low	1 - VL: Very Low	1 - VL: Very Low
LOSS QUESTION	What is the probable loss that will be incurred if an external attack is successful?	What is the probable loss if there are long-term communication outages?	What is the probable loss that will be incurred if an external attack is successful?	What is the probable loss that will be incurred if employees engage in malicious activity?	What is the probable loss that will be incurred if there is unauthorized access to ACH data?	What is the probable loss that will be incurred if ACH data is exposed?
PROBABLE LOSS	5 - VH: Very High	4 – H: High	5 - VH: Very High	5 - VH: Very High	5 - VH: Very High	5 - VH: Very High
RISK	3 - M: Moderate	2 – L: Low	3 - M: Moderate	3 - M: Moderate	3 - M: Moderate	3 - M: Moderate