SOUTHERN FINANCIAL EXCHANGE

Risks À la Carte

PICKING YOUR RISKS THE FFIEC WAY!

1

Disclaimers

- All opinions presented are my own and do not represent the opinions of ACH Alert or any other entity with which I have been, am now, or will be affiliated.
- The presentation and applicable materials are intended for general education purposes only and should not be considered legal, accounting, or tax advice
- You should consult your own attorney, accountant, or tax professional with any specific questions you may have related to this presentation that are of a legal, accounting, or tax nature
- Some of the opinions provided may not be the opinions of the presenter and are only provided to challenge existing thinking and reframe the participant's views around a specific subject

2

2

Menu

Preparing Risk Assessments
- Ingredients
- Recipes

The FFIEC Recipe
- Cybersecurity Framework Ingredients
- General Risk Assessment Ingredients
- FFIEC Recipes

3

3

Today's Chefs

David Payne, CIA, CFSA, AAP, NCP
Compliance Manager
Alkami Technology

Pam Rodriguez, AAP, CIA, CISA
SVP, Professional Services
Southern Financial Exchange

4

4

Risk Assessments Seen on the Menu

1. NIST Cybersecurity Framework
2. NIST SP 800-53
3. COSO
4. FFIEC Cybersecurity Framework
5. COBIT
6. ISO 27001
7. ISO 31000

5

Preparing Risk Assessments

ISSUES YOU MAY SEE WHEN DELIVERING A RISK ASSESSMENT ORDER

6

No Universal Recipes

ISO:

- the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence

NIST:

- IT-related risk;
  - the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and
  - the resulting impact if this should occur.

ISACA:

- The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise

7

7

Common Recipes

NIST

COBIT

ISA 62443-2

ISA 62443-3

ISO/IEC 27001

ISO 31000

8

8

How About the Cook

Quantitative
- Cook knows how to make the recipe
- May not measure ingredients

Qualitative
- Cook uses a recipe to make the recipe
- Measures everything out

9

9

Common Ingredients

Inherent Risk
- Uncontrolled risk

Mitigating Controls
- Actions taken to reduce inherent risk

Residual Risk
- Risk after factoring in mitigating controls

Future | Planned Risk
- A way of evaluating residual risk if additional mitigating controls are implemented
- Typically associated with areas of increased risk

10

10

Common Ingredients

Likelihood
- Chance of the risk occurring
- Used for both inherent and residual risk evaluation

Impact
- How much the risk will affect the organization
- Used for both inherent and residual risk evaluation

11

11

Common Ingredients

Velocity
- How quickly the impact of a potential risk will be felt by the organization

Duration
- Also referred to as Persistence
- How long the risk may impact the organization

12

12

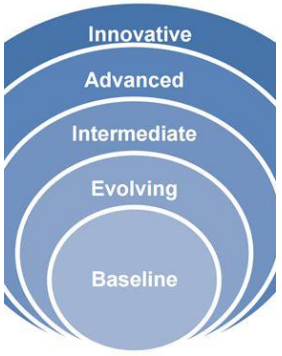
Common Ingredients

Threat
- External Threat – volume and type of attacks directed at the organization affect the FI's inherent risk

Vulnerability
- IT definition is not typically applied to risk assessments
- A weakness in a control may increase the organizations overall vulnerability to a potential risk

13

13

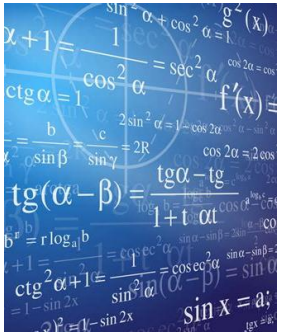


Common Ingredients

Control Maturity
- Method of rating the maturity of the control environment
- FFIEC Cybersecurity Assessment Tool
  - Baseline
  - Evolving
  - Intermediate
  - Advanced
  - Innovative

14

14



Measuring Amounts

ISO – Function of exploiting a Vulnerability measured by the Likelihood/Probability and Impact/Consequence

NIST – Likelihood/Probability and Impact/Consequence

Other Factors
- Velocity – how quickly the threat could occur
- Duration – how long the threat could last

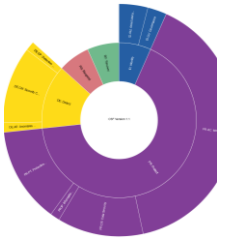
15

15

Measuring Amounts

How is it calculated?
- Likelihood/Probability * Impact/Consequence
- Likelihood/Probability * Impact/Consequence * Velocity
- Likelihood/Probability * Impact/Consequence * Velocity * Duration

How is it measured?
- 3 options – low, medium, & high
- 5 options – Minimal, Low, Medium, High, & Critical
- A mix between
  - Low, Medium, & High on Likelihood
  - Minimal, Low, Medium, High, & Critical on Impact



16

16

How do You Measure Risk?

1. Likelihood/Probability * Impact/Consequence
2. Likelihood/Probability * Impact/Consequence * Velocity
3. Likelihood/Probability * Impact/Consequence * Velocity * Duration
4. Other

17

17

Measuring Amounts

Qualitative Assessment

- What do the risk scores mean without an underlying "calculation"?

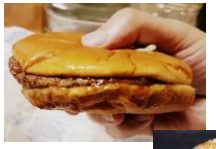
18

18

How Hungry are You?

Appetite
- How hungry you are?
- You'll eat more if you're hungry

Tolerance
- How willing you are to accept food that isn't "great"
- The hungrier you are the more likely you are to eat "fast" food
- You may even not notice if the food is "bad" and give you food poisoning



19

19

Replacing Ingredients

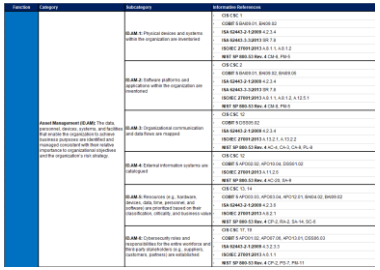
Review 2018-04-16_framework_v1.1_core1.xlsx mapping of NIST Cybersecurity Framework to:
- COBIT
- ISA 62443-2-1
- ISA 62443-3-3
- ISO/IEC 27001
- ISO 31000
- NIST SP 800-5

Visualization of COSO to NIST CSF
https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/othermapping/trust-services-map-to-nist-

Visualization of NIST CSF
https://csf.tools/csf-sunburst/csf.xlsx

20

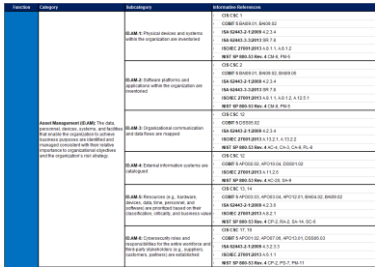
20



Replacing Ingredients

NIIST CSF Asset Management (ID.AM)

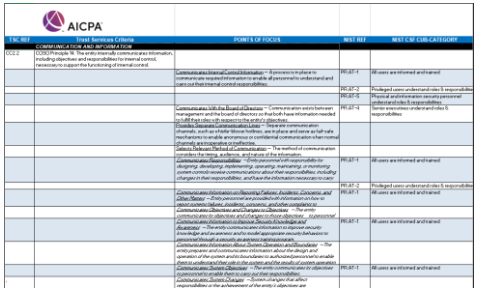
- ID.AM-1: Physical Devices & Systems within the organization are inventoried
  - CIS CSC 1
  - COBIT 5 BAI09.1, BAI09.02
  - ISA 62443-2-1:2009 4.2.3.4
  - ISA 62442-3-3:2013 SR 7.8
  - ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
  - NIST SP 800-53 Rev 4 CM-8, PM-5



Replacing Ingredients

NIIST CSF Asset Management (ID.AM)

- ID.AM-2: Software platforms and applications within the organization are inventoried
  - CIS CSC 2
  - COBIT 5 BAI09.1, BAI09.02, BAI09.5
  - ISA 62443-2-1:2009 4.2.3.4
  - ISA 62442-3-3:2013 SR 7.8
  - ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1
  - NIST SP 800-53 Rev 4 CM-8, PM-5



AICPA

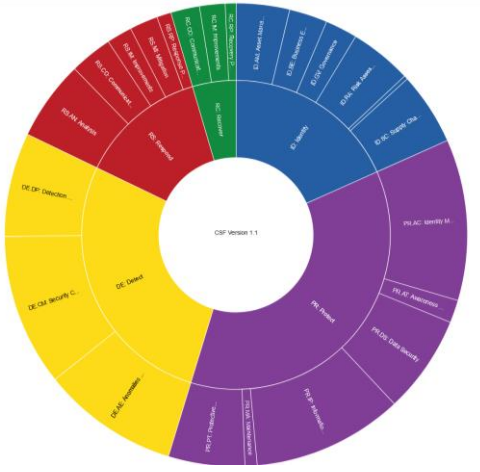
TSC REF	Trust Services Criteria	POINTS OF FOCUS	NIST REF	NIST CSF CUB-CATEGORY
	COMMUNICATION AND INFORMATION			
CC2.0	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
		Communicates Internal Control Information – A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.	PR.AT-1	All users are informed and trained
			PR.AT-2	Privileged users understand roles & responsibilities
			PR.AT-5	Physical and information security personnel understand roles & responsibilities
		Communicates With the Board of Directors – Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.	PR.AT-4	Senior executives understand roles & responsibilities
		Separate Communication Lines – Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.		
		Communication Protection and Storage – The method of communication considers the timing, audience, and nature of the information.		
		Communicates Responsibilities – Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.	PR.AT-1	All users are informed and trained
			PR.AT-2	Privileged users understand roles & responsibilities
		Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters – Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.	PR.AT-1	All users are informed and trained
		Communicates Objectives and Changes to Objectives – The entity communicates its objectives and changes to those objectives to personnel in a timely manner using established communication channels.		
		Communicates Information to Improve Security Knowledge and Awareness – The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.	PR.AT-1	All users are informed and trained
		Communicates Information About System Operation and Boundaries – The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.		
		Communicates System Objectives – The entity communicates its objectives to personnel to enable them to carry out their responsibilities.	PR.AT-1	All users are informed and trained
		Communicates System Changes – System changes that affect responsibilities or the achievement of the entity's objectives are		

Replacing Ingredients

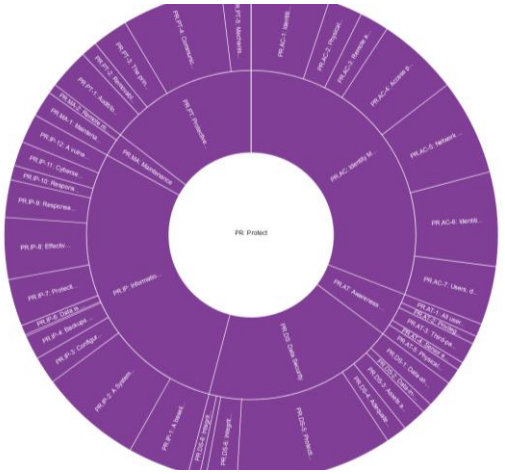
COSO to NIST CSF Mapping

- Principle 14: Communicates Internal Control Information
  - PR.AT-1 All users are informed and trained
  - PR.AT-2 Privileged users understand roles & responsibilities
  - PR.AT-5 Physical and information security personnel understand roles & responsibilities
- Principle 14: Communicates With the Board of Directors
  - PR.AT-4 Senior executives understand roles & responsibilities

NIST CSF Visualization



NIST CSF Visualization



25

25

The FFIEC Recipe

WHAT ARE WE MAKING?

26

26

Cybersecurity Framework Ingredients

FFIEC to NIST CSF

Review mapping of FFIEC to NIST
https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf

FFIEC IT EXAMINATION HANDBOOK INFOBASE

27

27

General Risk Assessment Ingredients

Strategic
- Opt-in/Opt-out perspective

Reputation
- Opt-in/Opt-out perspective

Credit
- Credit Push (Wire, RTP, ACH)
- Debit Pull (ACH)
- Check deposit (Mobile | Remote)

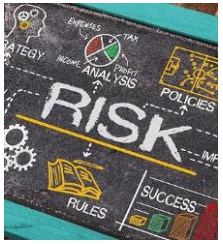
28

28

General Risk Assessments Ingredients

Liquidity
- Not included in most payment system risk assessments
- FI's perspective
- Customer's perspective

Operational
- Internal & Operational Controls
- Audit
- Information Security
- Business Continuity Planning
- Vendor & Third-Party Management



29

29

General Risk Assessments Ingredients

Legal/Compliance
- Uniform Commercial Code 3 & 4
- Regulation CC
- Regulation E
- Regulation J
- Nacha Operating Rules
- ECCHO Rules
- Gramm Leach Bliley Act
- Bank Secrecy Act
- Office of Foreign Assets Control
- Federal Reserve Operating Circulars

30

30

FFIEC Recipes

IT Booklets

Audit	Operations
Business Continuity Management	Outsourcing Technology Services
Development and Acquisition	Retail Payment Systems
E-Banking	Supervision of Technology Service Providers
Information Security	Wholesale Payment Systems
Management	Archived Booklets

31

31

FFIEC Recipes

Information Security IT Examination Handbook

- Threats references the National Institute of Standards and Technology (NIST)
- Risk Measurement
  - Cybersecurity Assessment Tool
  - References the NIST Cybersecurity Framework
- Risk Mitigation
  - Internal Controls

- II Information Security Program Management
  - II.A Risk Identification
    - II.A.1 Threats
    - II.A.2 Vulnerabilities
    - II.A.3 Supervision of Cybersecurity Risk and Resources
      - II.A.3(a) Supervision of Cybersecurity Risk
      - II.A.3(b) Resources for Cybersecurity Preparedness
  - II.B Risk Measurement
  - II.C Risk Mitigation
    - II.C.1 Policies, Standards, and Procedures
    - II.C.2 Technology Design
    - II.C.3 Control Types
    - II.C.4 Control Implementation

32

32

FFIEC Recipes

Operations IT Examination Handbook

Risk Assessment

Action Summary

Management should analyze the survey of the IT operations environment and the inventory of technology resources to identify threats and vulnerabilities to IT operations. The assessment process should identify:

- Internal and external risks;
- Risks associated with individual platforms, systems, or processes as well as those of a systemic nature; and
- The quality and quantity of controls.

To the extent possible, the assessment process should quantify the probability of a threat or vulnerability and the financial consequences of such an event.

33

33

FFIEC Recipes

Operations IT Examination Handbook

- Risk Identification
  - Environmental Survey
  - Technology Inventory
    - Hardware
    - Software
    - Network Components and Topology
    - Media
- **Risk Assessment**
  - Prioritizing Risk Mitigation Efforts
- Risk Mitigation and Control Implementation
  - Policies, Standards, and Procedures
    - Policies
    - Standards
    - Procedures
  - Controls Implementation
    - Environmental Controls
    - Preventive Maintenance

34

34

Payment System Risk Recipes

Unauthorized Access
- Wire Transfer
- Real Time Payment
- Debit Card
- Credit Card
- Automated Clearing House
- Checks

Returns
- Automated Clearing House
  - Reclamations (ACH)
- Check Deposits
  - Branch
  - ATM
  - Mobile
  - RDC

Team Building

COOKING WITH RISK

Recipe #1 Ingredients

File Transmission
- ACH Operator is Fed
- Sending and Receiving point is a Third-Party
- Settlement point is the Fed

Originator Analysis
- 795 Originator
- 1 TPS with 117 Originators (property management company sending debits nationally)
- SEC Codes – PPD, CCD, CTX
- Volume is high, both dollars and items
- FI customers have international ties
- FI does not send IATs

37

Recipe #1 Ingredients

Internal Environment
- Strong internal controls
- Policies are board-approved
- Detailed procedures
- Well-trained staff
- Daily reports are reviewed
- Files and file totals are verified prior to releasing for processing
- System limits
- Dual control
- Exposure limits reviewed monthly
- Return activity reviewed monthly

38

Recipe #1 Ingredients

Online Banking
- All products are offered to customers
- Limits are reasonable
- Additional mitigating controls are in place

Agreement Analysis
- Originator & TPS agreements are strong
- Some older agreements
- TPS customer agreement are strong

39

Recipe #1 Ingredients

Compliance Environment
- CIP program
- Thorough onboarding process
- Periodic reviews are based on customer's risk
- Process documented
- Anomaly monitoring in place
- Effective BSA, AML, OFAC, Information Security and Technology programs in place

40

Recipe #1 Ingredients

Audit Analysis
- Audits & Risk Assessments are consistently performed
- Third-Party Service Provider ACH compliance audit verified
- Proof of audit and risk assessment requested from Third-Party Sender
  - TPS did not provided either
- One finding:
  - TPS agreement with their clients
- Three compliant with exceptions:
  - Third-Party Sender audit missing
  - Authorizations missing information
  - Originator and Third-Party Sender training
- Exposure Limits:
  - Limits are set and are periodically reviewed
  - A few of the customers reviewed appear to have higher limits than needed based on activity

41

41

Risk #1

THERE IS A RISK THE ORIGINATOR IS UNABLE TO EFFECTIVELY MANAGE THEIR ACH ORIGINATION ACTIVITY.

42

42

Risk #1

What do you think the residual risk is for this institution?

1. Low
2. Medium
3. High

43

Risk #2

THERE IS A RISK OF RECEIVING A FRAUDULENT ACH TRANSFER REQUEST.

44

Risk #2

1. Low
2. Medium
3. High

45

Risk #3

THERE IS A RISK OF NACHA ASSESSING A FINE FOR NON-COMPLIANCE.

46

Risk #3

1. Low
2. Medium
3. High

47

Questions

48

Contact Information

David Payne
Compliance Manager
Alkami Technology
david.payne@alkami.com

Pam Rodriguez
SVP, Professional Services
Southern Financial Exchange™
prodriguez@sfe.org