



The Information Security Experts



Best Practices in IT Governance

Erik Petersen, VP of Professional Services

Agenda

Governance Issues

- Goal of Governance for IT Controls—Effectiveness Perspective
- Regulatory Expectations for Governance
- Best Practice Governance Model
- Run through with the new FDIC Questionnaire

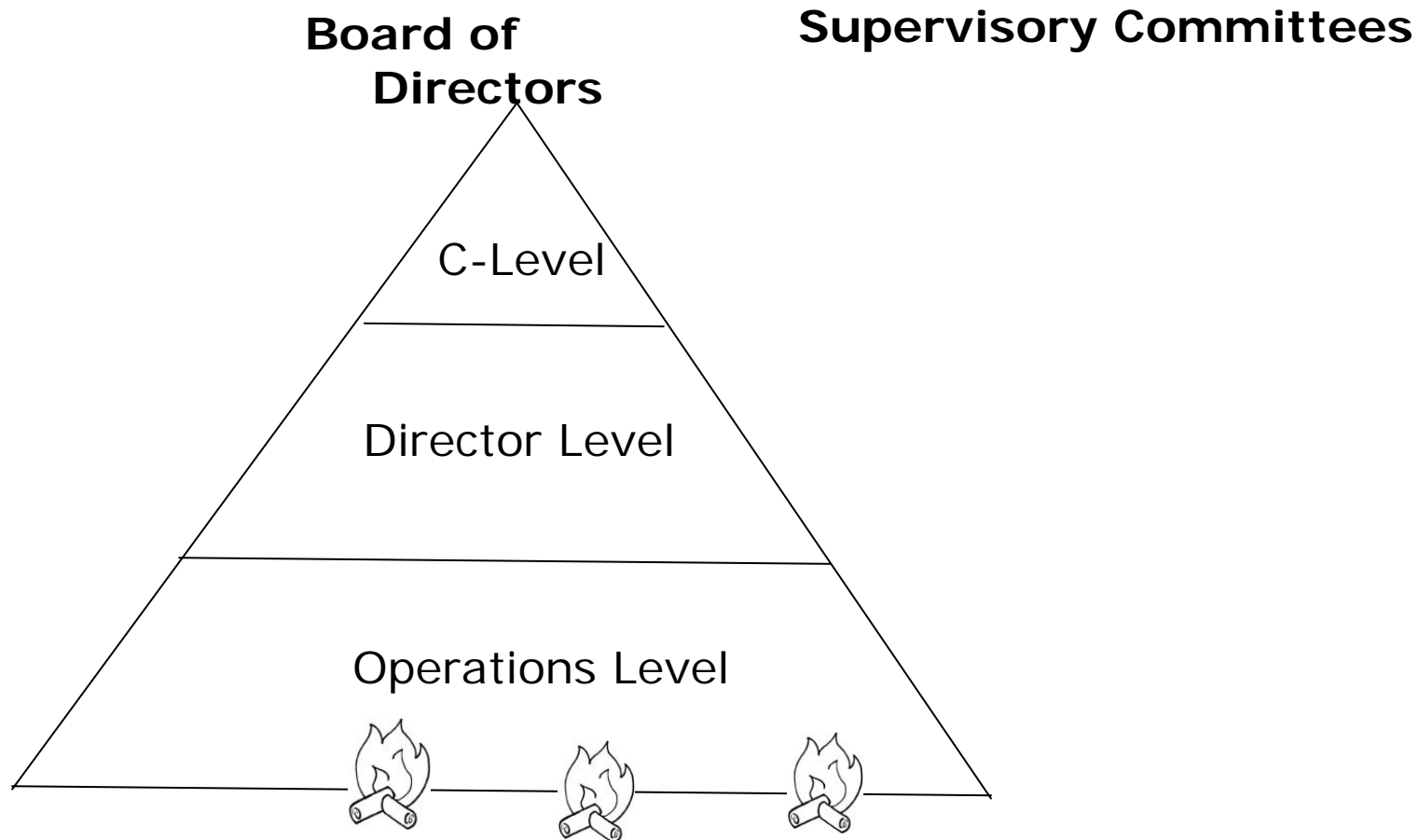
Emerging Issues

- IT Controls and M+A
- Diligence and Deal Books

Q and A

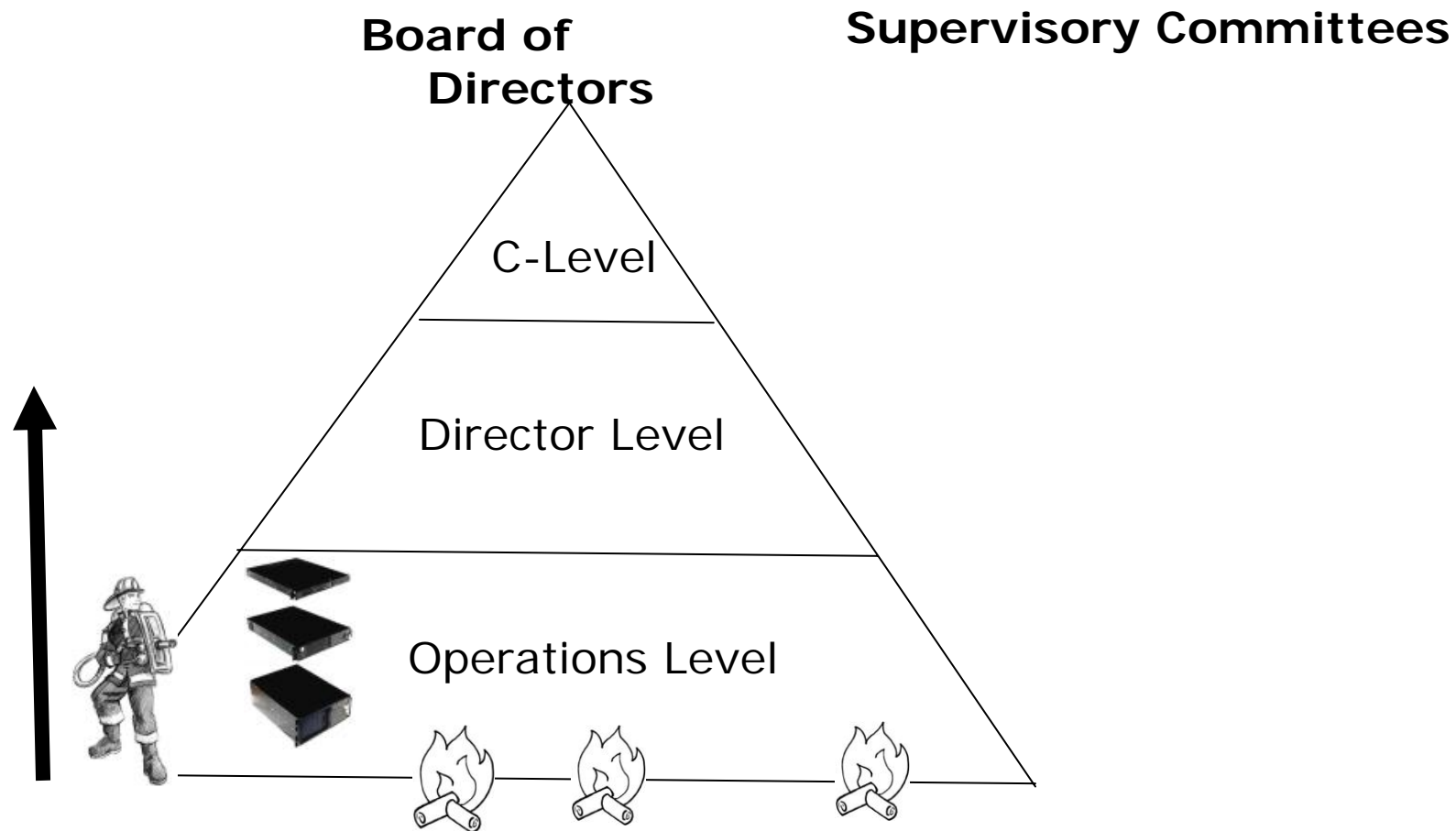
Historical “Governance” Model for IT Controls

--*Bottom Up, Reactive*

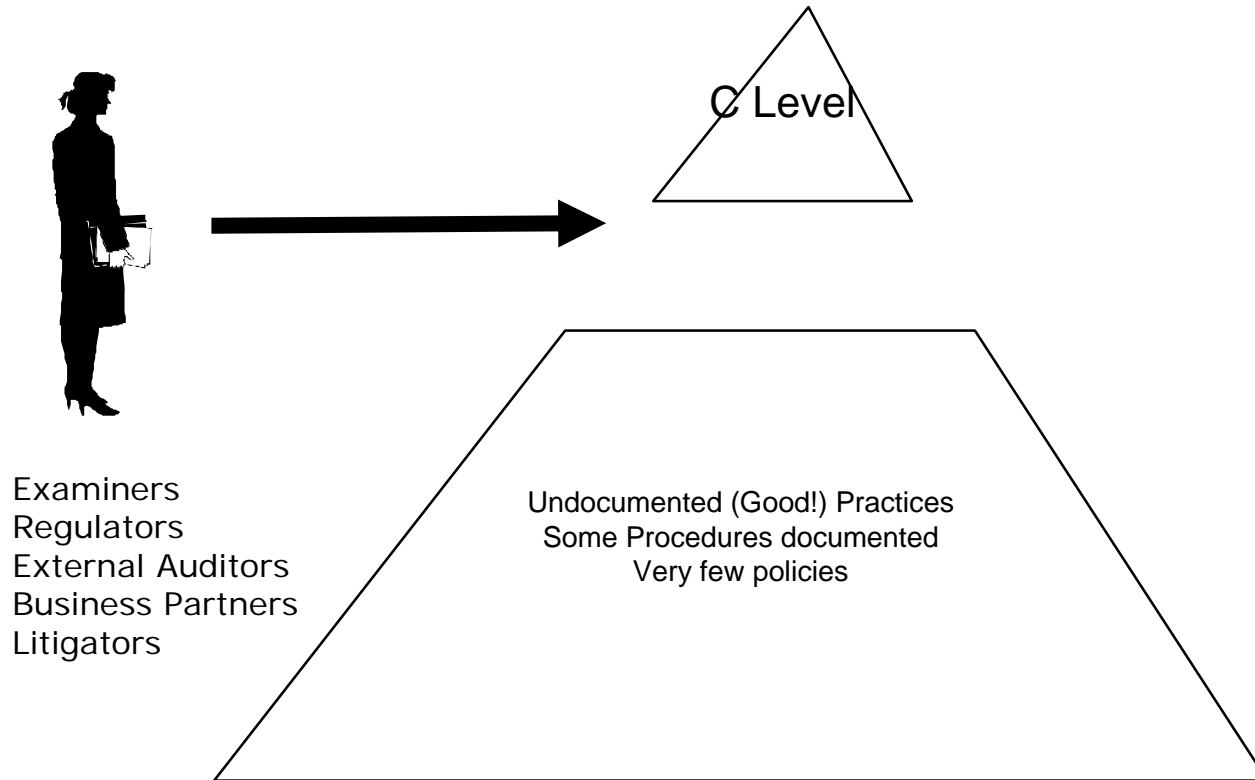


Historical Model for Security

--*Bottom Up, Reactive*

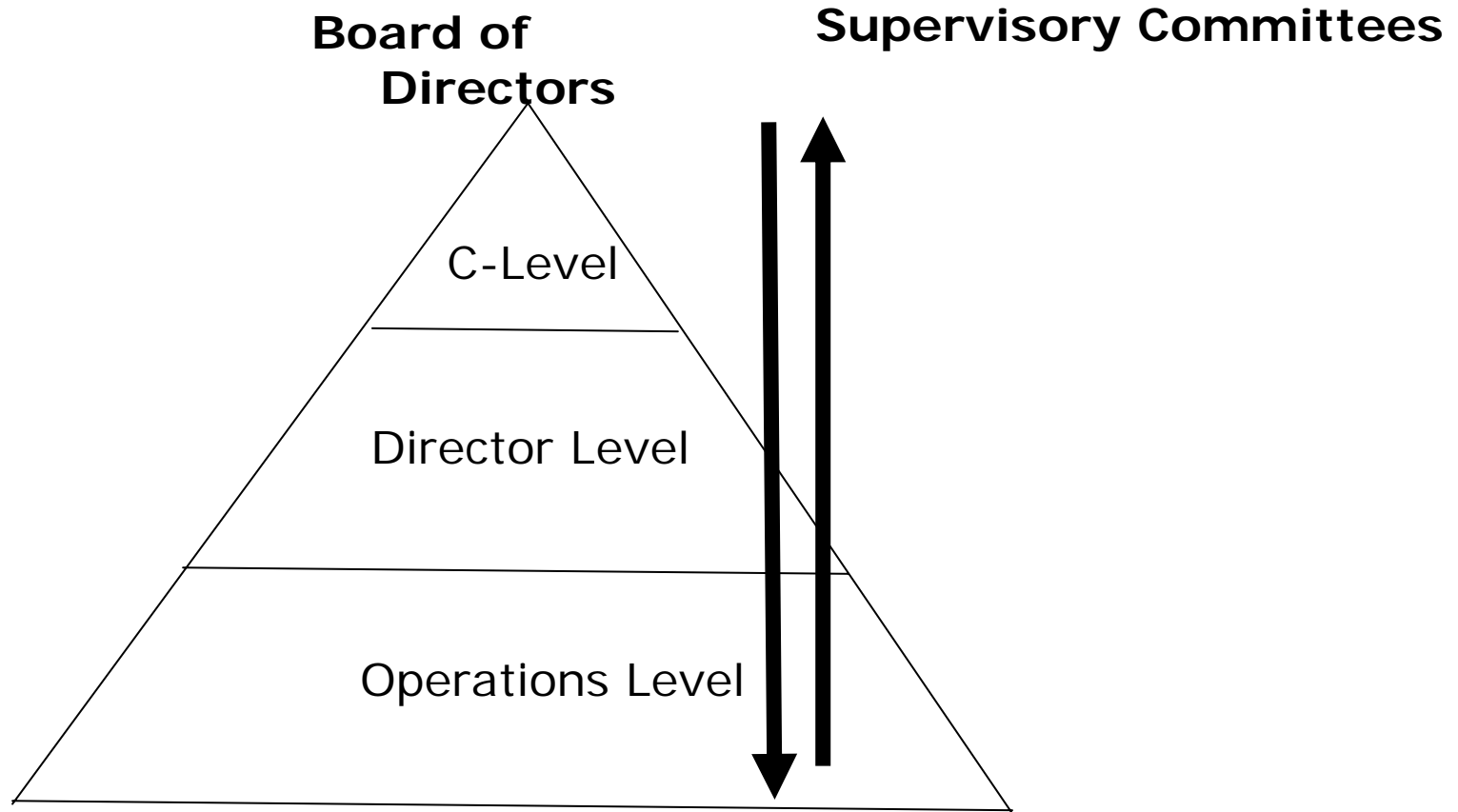


3rd Party Problem

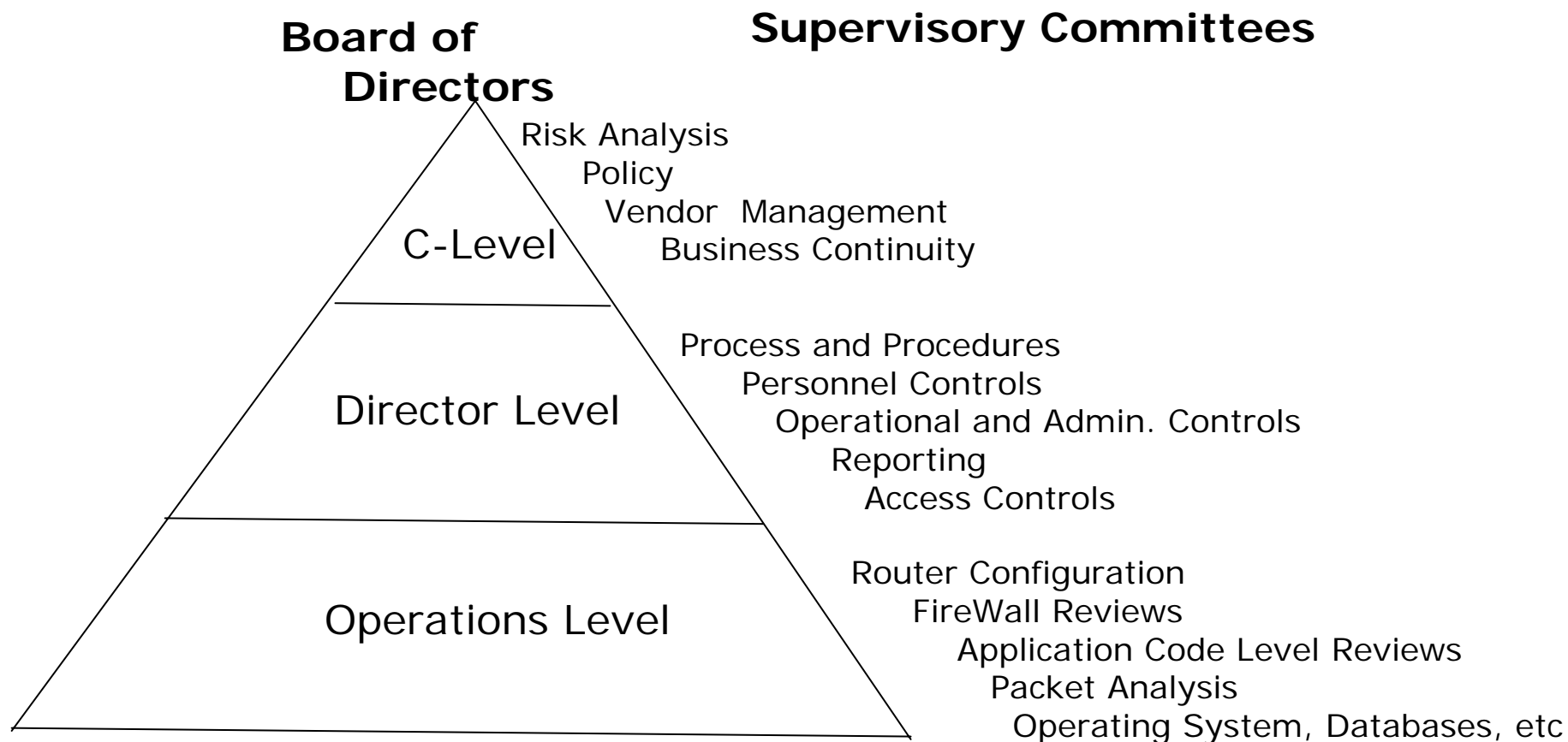


Governance Model for IT Controls

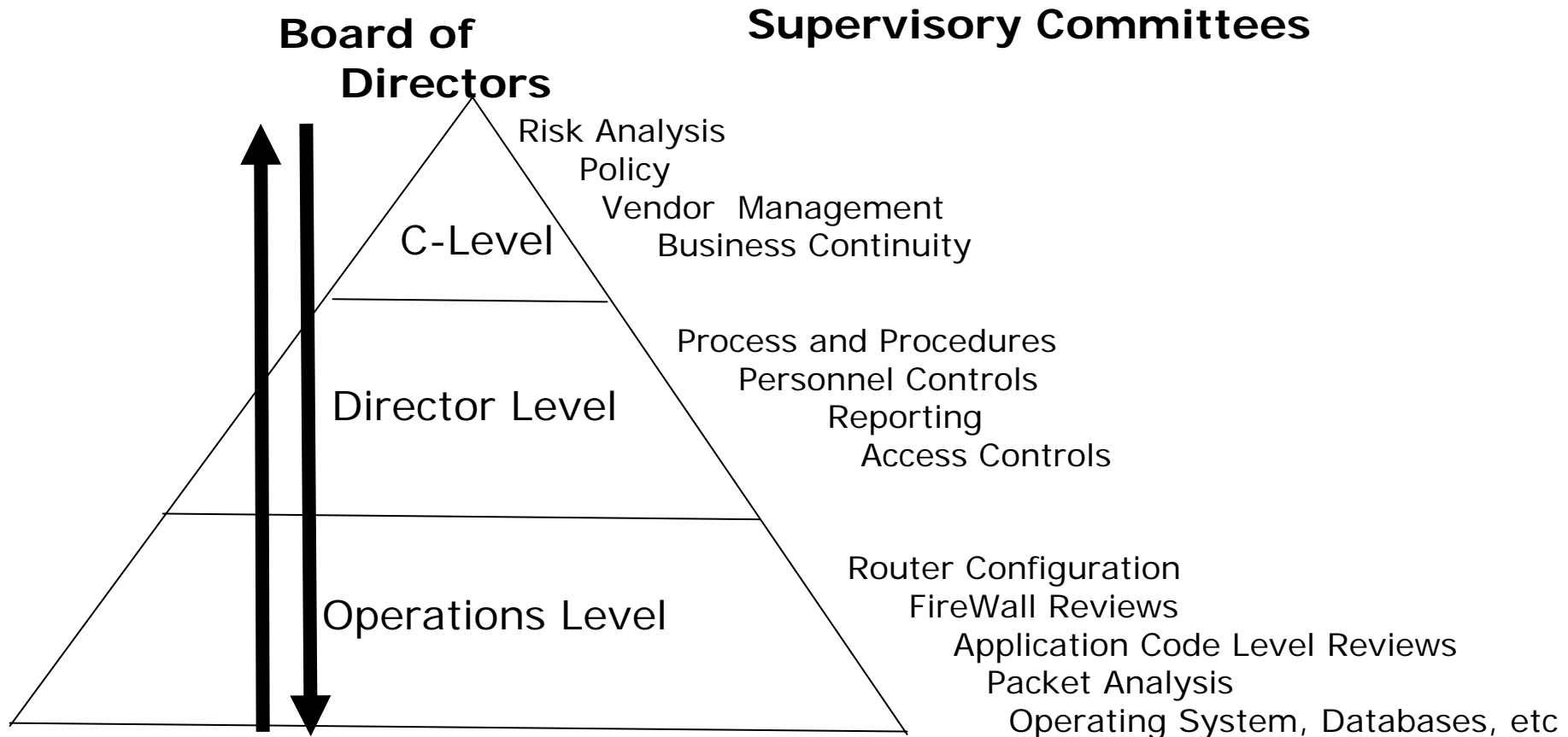
--*Top Down (or “integrated”)*



Goal is Governance structure that maps into the organization, without burdening Board



And fully integrated: Top down/bottom up





Regulatory Expectations

Board and GLB A and IT Controls

Examination Expectations *(from FFIEC "Management" Handbook):*

1. "The board is responsible for **overseeing and approving** the development, implementation, and maintenance of a comprehensive, **written information security program**, as required by the Gramm-Leach-Bliley Act (GLBA)".
--And that--
2. "that it [Board] **assigns specific responsibility** for its implementation.

Board and Internal IT Audit

Examination Expectations *(from FFIEC "Audit" Handbook):*

1. "The board of directors has overall responsibility for the effectiveness of the audit function."
2. "The board of directors and senior management are responsible for **providing the audit function** with sufficient resources to ensure **adequate IT coverage** and audit function independence."

Board and IT Governance

Examination Expectations *(from FFIEC "Management" Handbook):*

1. The board may delegate information security monitoring to an **independent audit function**...
2. .. and information security management to an independent function.
3. Ideally, the institution **should separate** information security **program management** and monitoring from the daily security duties required in **IT operations**.
4. Boards of directors should establish IT oversight by ensuring **strong board involvement and awareness of IT activities**



Best Practice Model

Board of Directors

Audit Committee

Exam Results
(sometimes
require BoD
action)

FDIC
FRB
OCC
OTS



Independent
Reports and Test
Results

3rd
Party



**Regulatory
Exam
And
Independent
3rd Party**

Yearly Report

CISC
Chair=CFO?

InfoSec Program

IT Policies

Security Standards

Interpret

Grant Waivers

3rd Party Testing (pen
tests, etc)

**Information
Security
Management**

Yearly Report

Tech Steering Committee
Chair=CIO

Maintain IT Strategic Plan

Monitor major IT projects

Coordinate priorities between IT
and user departments

Review adequacy and allocation
of IT resources

IT Operations

Audit Results
Audit Plans
Etc.

Independent IT
audits

Test IT Controls

Maintain risk based
Audit Plan

Follow up

**Internal
Audit**



New FDIC IT Examination Questionnaire

New FDIC Questionnaire

I hereby certify that the following statements are true and correct to the best of my knowledge and belief.

Officer's Name and Title

Institution's Name and Location

Officer's Signature

Date Signed

As of Date

This is an official document. Any false information contained in it may be grounds for prosecution and may be punishable by fine or imprisonment.

Board of Directors

Audit Committee

Exam Results
(sometimes require BoD action)

FDIC
FRB
OCC
OTS



Independent Reports and Test Results

3rd Party



Regulatory Exam
And
Independent
3rd Party

Yearly Report

CISC
Chair=CFO?

InfoSec Program

IT Policies

Security Standards

Interpret

Grant Waivers

3rd Party Testing (pen tests, etc)

Information Security Management

Yearly Report

Tech Steering Committee
Chair=CIO

Is your risk assessment program formally approved by the Board of Directors at least annually (Y/N)?

[FDIC Rules and Regulations Part 364 Appendix B Section III (A)(1) and (F)]

Review adequacy and allocation of IT resources

IT Operations

Audit Results
Audit Plans
Etc.

Independent IT audits

Test IT Controls

Maintain risk based Audit Plan

Follow up

Internal Audit

Board of Directors

Audit Committee

Exam Results
(sometimes require BoD action)

FDIC
FRB
OCC
OTS



Independent Reports and Test Results

3rd Party



Regulatory Exam And Independent 3rd Party

Yearly Report

CISC
Chair=CFO?

InfoSec Program

IT Policies

Security Standards

Interpret

Grant Waivers

3rd Party Testing (pen tests, etc)

Information Security Management

Yearly Report

Tech Steering Committee
Chair=CIO

Has a report of risk assessment findings been presented to the Board of Directors for review and acceptance (Y/N)?

[FDIC Rules and Regulations Part 364 Appendix B Section III (F)]

Coordinate priorities between IT and user departments

Review adequacy and allocation of IT resources

IT Operations

Audit Results
Audit Plans
Etc.

Maintain risk based Audit Plan

Follow up

Internal Audit

Board of Directors

Audit Committee

Exam Results
(sometimes require BoD action)

Yearly Report

Yearly Report

Audit Results
Audit Plans
Etc.

FDIC
FRB
OCC
OTS



Independent
Reports and Test
Results

3rd
Party



Regulatory
Exam
And
Independent
3rd Party

CISC

Chair=CFO?

Tech Steering Committee

Chair=CIO

InfoSec Program

IT Policies

Security Standards

Interpret

Grant Waivers

3rd Party Testing (pen tests, etc)

Information
Security
Management

Do you have a written information security program designed to manage and control risk (Y/N)?

[FDIC Rules and Regulations Part 364 Appendix B Section II (A) and Section III (C)(1)]

If "Yes," please provide the date that the written information security program was last approved by the Board of Directors:

[FDIC Rules and Regulations Part 364 Appendix B Section III (A)(1)]

IT Operations

Internal
Audit

Board of Directors

Audit Committee

Exam Results
(sometimes
require BoD
action)

Yearly Report

Yearly Report

Audit Results
Audit Plans

FDIC
FRB
OCC
OTS



Independent
Reports and Test
Results

3rd
Party



**Regulatory
Exam
And
Independent
3rd Party**

CISC
Chair=CFO?

InfoSec Program

IT Policies

Security Standards

Interpret

Grant Waivers

3rd Party Testing (pen
tests, etc)

**Information
Security
Management**

Does your information security program contain written policies, procedures, and guidelines for securing, maintaining, and monitoring the following systems or platforms:

- [
- Core banking system (Y/N)?
- Imaging (Y/N)?
- Remote deposit capture (Y/N)?
- Payment systems (including wire transfer and ACH) (Y/N)?
- Voice over IP telephony (Y/N)?
- Instant messaging (Y/N)?
- Virtual private networking (Y/N)?
- Wireless networking - LAN or WAN(Y/N)?
- Local area networking (Y/N)?
- Wide area networking (Y/N)?
- Routers (Y/N)?
- Modems or modem pools (Y/N)?
- Security devices such as firewall(s) and proxy devices. (Y/N)?
- Other remote access connectivity such as GoToMyPC, PcAnywhere, etc. (Y/N)?
- Portable devices such as PDAs, laptops, cell phones, etc. (Y/N)?
- Other – please list:

FFIEC IT Examination Handbook, Information Security Booklet; FIL-12-1999 Uniform Rating System for Information Technology]

Board of Directors

Audit Committee

Exam Results
(sometimes require BoD action)

Yearly Report

Yearly Report

Audit Results
Audit Plans
Etc.

FDIC
FRB
OCC
OTS



Independent
Reports and Test
Results

3rd
Party



**Regulatory
Exam
And
Independent
3rd Party**

CISC
Chair=CFO?

Please provide the names and titles and/or committee members charged with formally overseeing and implementing the information security program:

[FDIC Rules and Regulations Part 364 Appendix B Section II (A) and Section III (A)(2)]

InfoSec Program

IT Policies

Security Standards

Interpret

Grant Waivers

3rd Party Testing (pen tests, etc)

**Information
Security
Management**

Monitor major IT projects

Coordinate priorities between IT and user departments

Review adequacy and allocation of IT resources

IT Operations

Test IT Controls

Maintain risk based Audit Plan

Follow up

**Internal
Audit**

Board of Directors

Audit Committee

Exam Results
(sometimes require BoD action)

FDIC
FRB
OCC
OTS



Independent Reports and Test Results

3rd Party



Regulatory Exam And Independent 3rd Party

Yearly Report

CISC
Chair=CFO?

InfoSec Program

IT Policies

Security Standards

Interpret

Grant Waivers

3rd Party Testing (pen tests, etc)

Information Security Management

Yearly Report

Does the bank report the overall status of the information security program and compliance with the Interagency Guidelines Establishing Information Security Standards to the Board or designated committee (Y/N)?
[FDIC Rules and Regulations Part 364 Appendix

and user departments

Review adequacy and allocation of IT resources

IT Operations

Audit Results
Audit Plans
Etc.

Maintain risk based Audit Plan
Follow up

Internal Audit

Board of Directors

Audit Committee

Exam Results
(sometimes require BoD action)

FDIC
FRB
OCC
OTS



Independent Reports and Test Results

3rd Party



Yearly Report

CISC
Chair=CFO?

InfoSec Program

IT Policies

Security Standards

Interpret

Information Security Management

Yearly Report

Tech Steering Committee
Chair=CIO

Maintain IT Strategic Plan

Monitor major IT projects

Coordinate priorities between IT

departments

and allocation

resources

IT Operations

Audit Results
Audit Plans
Etc.

Independent IT audits

Test IT Controls

Maintain risk based Audit Plan

Follow up

Internal Audit

Does the bank's strategic planning process incorporate information security (Y/N)?

[FFIEC IT Examination Handbook, Management Booklet]

Section

Regu
Exam

And
Independent
3rd Party

Board of Directors

Audit Committee

Exam Results
(sometimes require BoD action)

Yearly Report

Yearly Report

Audit Results
Audit Plans
Etc.

FDIC
FRB
OCC
OTS



CISC
Chair=CFO?

Tech Steering Committee
Chair=CIO

Independent Reports and Test Results

InfoSec Program

Please provide the following information regarding your most recent IT audits/independent reviews:

[FDIC Rules and Regulations Part 364 Appendix B Section III (C)(3) and (F); FFIEC IT Examination Handbook, Audit Booklet; FIL-12-1999 Uniform Rating System

3rd Party



Regulatory Exam And Independent 3rd Party

	Audit Date	Entity Conducting Audit	Written Audit Report (Y/N)	Audit Committee/Board Review Date
Information Security Program				
IT General Controls Review				
Vulnerability Testing				
Penetration Testing				
Wire Transfer Audit				
NACHA Rule Compliance Audit				

Independent IT audits

Controls

risk based
t Plan

ow up

Internal
Audit

Board of Directors

Audit Committee

Exam Results
(sometimes require BoD action)

Yearly Report

Yearly Report

Audit Results
Audit Plans
Etc.

FDIC
FRB
OCC
OTS



CISC
Chair=CFO?

Tech Steering Committee
Chair=CIO

Independent Reports and Test Results

3rd Party



InfoSec Program

IT Policies

Security Standards

Maintain IT Strategic Plan

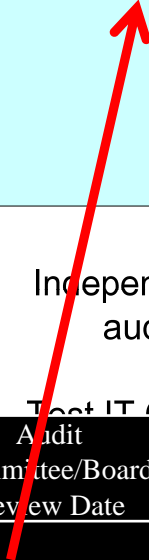
Monitor major IT projects

Independent IT audits

Test IT Controls

Regulatory Exam And Independent 3rd Party

	Audit Date	Entity Conducting Audit	Written Audit Report (Y/N)	Audit Committee/Board Review Date
Information Security Program		Internal Audit or 3 rd Party		
IT General Controls Review				
Vulnerability Testing				
Penetration Testing				
Wire Transfer Audit				
NACHA Rule Compliance Audit				



3^r

Task based Plan
Group
Annual Audit

Board of Directors

Audit Committee

Yearly Report

Yearly Report

Audit Results
Audit Plans
Etc.

CISC
Chair=CFO?

Tech Steering Committee
Chair=CIO

InfoSec Program

IT Policies

Security Standards

Interpret

Maintain IT Strategic Plan

Monitor major IT projects

Coordinate priorities between IT

Independent IT
audits

Test IT Controls

	Audit Date	Entity Conducting Audit	Written Audit Report (Y/N)	Audit Committee/Board Review Date	risk based Audit Plan
Information Security Program					Follow up
IT General Controls Review		Internal Audit or 3 rd Party			
Vulnerability Testing					
Penetration Testing					Internal Audit
Wire Transfer Audit					
NACHA Rule Compliance Audit					

Exam Results
(sometimes
require BoD
action)

FDIC
FRB
OCC
OTS



Independent
Reports and Test
Results

3rd
Party



**Regulatory
Exam
And
Independent
3rd Party**



Board of Directors

Audit Committee

Exam Results
(sometimes require BoD action)

Yearly Report

Yearly Report

Audit Results
Audit Plans
Etc.

FDIC
FRB
OCC
OTS



CISC
Chair=CFO?

Tech Steering Committee
Chair=CIO

Independent Reports and Test Results

InfoSec Program

IT Policies

Security Standards

Interpret

Maintain IT Strategic Plan

Monitor major IT projects

Coordinate priorities between IT

Independent IT audits

Test IT Controls

3rd Party



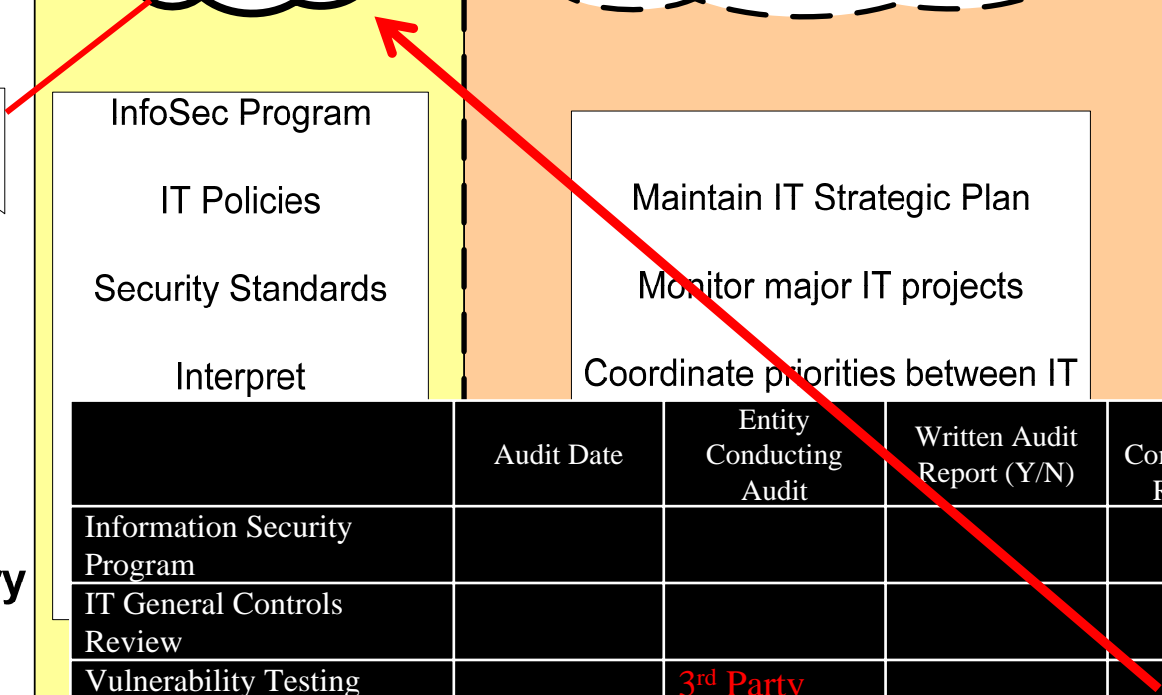
	Audit Date	Entity Conducting Audit	Written Audit Report (Y/N)	Audit Committee/Board Review Date
Information Security Program				
IT General Controls Review				
Vulnerability Testing		3 rd Party		
Penetration Testing		3 rd Party		
Wire Transfer Audit				
NACHA Rule Compliance Audit				

risk based
t Plan

ow up

ernal
udit

Regulatory Exam And Independent 3rd Party



Board of Directors

Audit Committee

Exam Results
(sometimes require BoD action)

Yearly Report

Yearly Report

Audit Results
Audit Plans
Etc.

FDIC
FRB
OCC
OTS



CISC
Chair=CFO?

Tech Steering Committee
Chair=CIO

Independent Reports and Test Results

3rd Party



InfoSec Program

IT Policies

Security Standards

Interpret

Maintain IT Strategic Plan

Monitor major IT projects

Coordinate priorities between IT

Independent IT audits

Test IT Controls

	Audit Date	Entity Conducting Audit	Written Audit Report (Y/N)	Audit Committee/Board Review Date
Information Security Program				
IT General Controls Review				
Vulnerability Testing				
Penetration Testing				
Wire Transfer Audit		Internal Audit		
NACHA Rule Compliance Audit		Internal Audit		

risk based
t Plan

ow up

Internal
Audit

Regulatory Exam
And
Independent
3rd Party



Yearly Checklist

- ✓ Risk Assessment PROGRAM Reviewed
- ✓ Risk Assessment FINDINGS reviewed
- ✓ Information Security Program reviewed
- ✓ Summary of Compliance with Interagency Guidelines
- ✓ Audit/Independent Results Review
 - From Audit
 - Information Security Program Review
 - General Controls Review
 - Wire Transfer
 - NACHA
 - From CISC
 - Vulnerability Testing Results
 - Penetration Tests
- ✓ From Tech Steering Committee
 - Review IT Strategic Plan
 - Information Security Strategic Plan



Emerging Issues for Boards to Consider

Emerging Board Governance Issues

Merger and Acquisition--*IT Controls should be considered.*

If one entity has advanced capability maturity, and the other is immature...what should happen post deal? One month out? 2 months out? 1 year?

- Add IT Controls request to diligence package
- Assign Controls section to someone outside of IT if possible.
- Deal book to board should identify costs, and financial synergies post-deal.
- Each cost or synergy should be assigned, along with timelines.

IT Controls Diligence—Deal Book

A. Diligence Objectives

B. Due Diligence Activities and Key Findings

___ Due Diligence Activities

___ Key Findings

C. Comparison of Cultures

D. Professional Certifications and Development

E. Formal IT Controls Capabilities Delivered

F. Comparison of IT Controls Maturity Levels

G. Senior Management

H. Key Employees

I. Assessment of Potential “Brain Drain” from Staff Losses

J. Examination and Incident History

K. Synergies and New Opportunities

___ Cost Saving Synergies

___ Revenue Synergies

L. Risks and Effects of the Merger

___ Risks

___ Budget Effects

M. Integration and Risk Mitigation Plan

___ Integration Plan—KEY ELEMENT!

___ Risk Mitigation Plan

N. New Org Chart

O. Recommendations to Board

SecureWorks®

Questions?