Data Flow Diagramming

for those of us who thought we'd never need to!

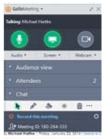
Dan Hadaway, CRISC

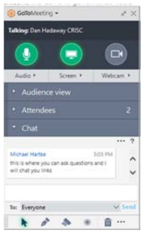
infotex 15
est. 2000

Welcome

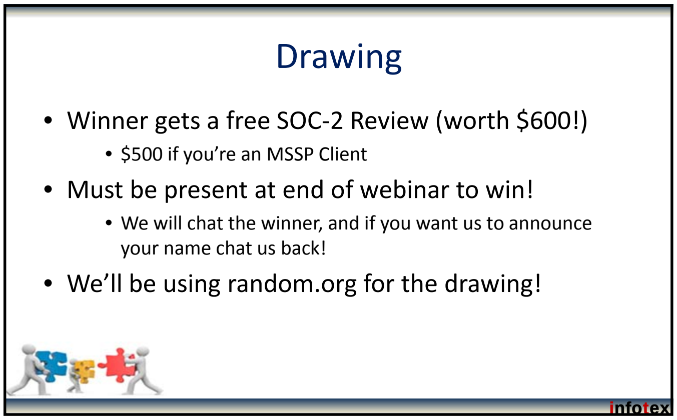
Housekeeping

- I'm Michael Hartke . . . .
- If you have questions . . . .
- I will chat you links . . . .





Michael Hartke 5:03 PM
this is where you can ask questions and I will chat you links



Drawing

- Winner gets a free SOC-2 Review (worth $600!)
  - $500 if you're an MSSP Client
- Must be present at end of webinar to win!
  - We will chat the winner, and if you want us to announce your name chat us back!
- We'll be using random.org for the drawing!

Educational Series

- my.infotex.com/the-2016-it-governance-tour

Highlighted Webinar

- Simplifying the Incident Response
  - Put your management team in a position where when (and no longer if) the career threatening event occurs, they recognize the process as you unfold it.
  - April 12th Yes, we've been known to move these!
  - **Free!**

Technology
People
Policy
Process

dan hadaway

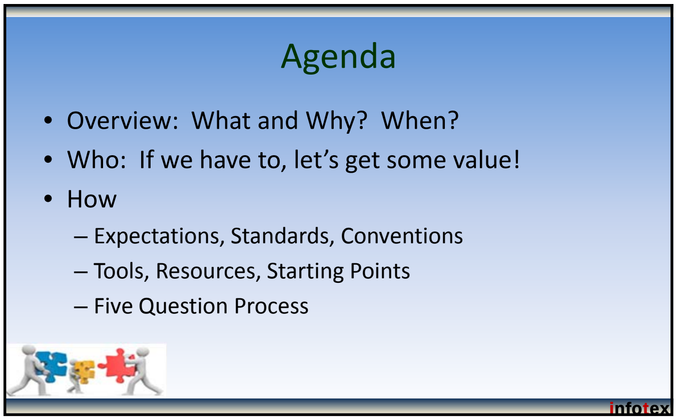
Managing Partner, infotex

infotex

First of all . . . .

infotex

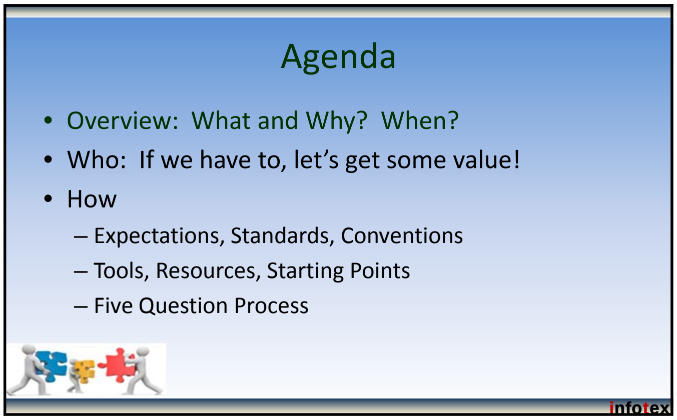
infotex



Agenda

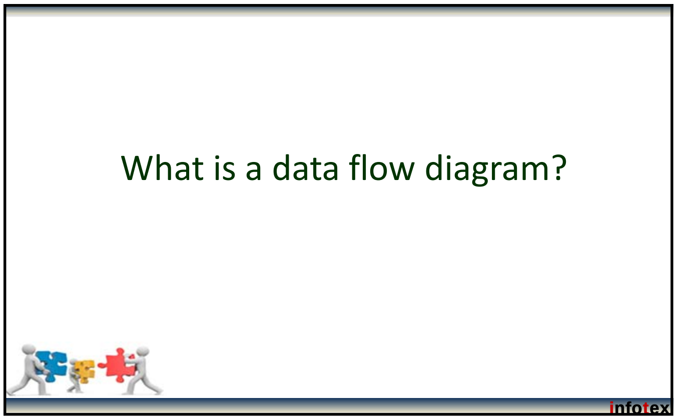
- Overview: What and Why? When?
- Who: If we have to, let's get some value!
- How
  - Expectations, Standards, Conventions
  - Tools, Resources, Starting Points
  - Five Question Process

infotex

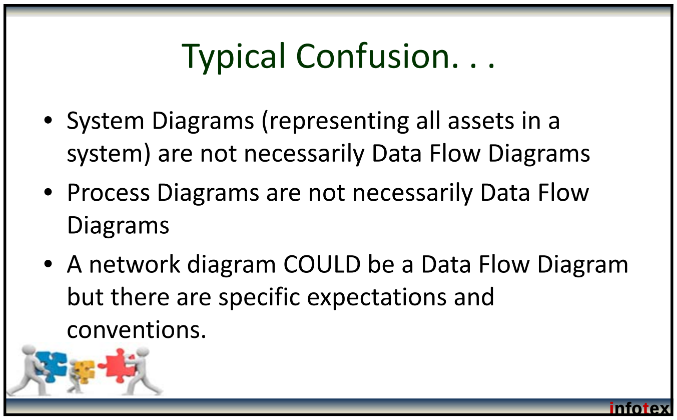


Agenda

- Overview: What and Why? When?
- Who: If we have to, let's get some value!
- How
  - Expectations, Standards, Conventions
  - Tools, Resources, Starting Points
  - Five Question Process



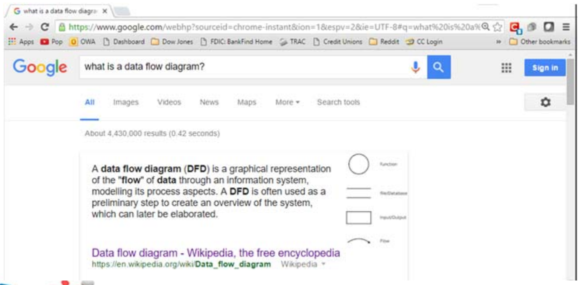
What is a data flow diagram?



Typical Confusion. . .

- System Diagrams (representing all assets in a system) are not necessarily Data Flow Diagrams
- Process Diagrams are not necessarily Data Flow Diagrams
- A network diagram COULD be a Data Flow Diagram but there are specific expectations and conventions.

What?


what is a data flow diagram?
https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=what%20is%20a%
Apps Pop OWA Dashboard Dow Jones FDIC: BankFind Home TRAC Credit Unions Reddit CC Login Other bookmarks
Google
Sign in
All Images Videos News Maps More Search tools
Function
File/Database
Input/Output
Flow

what is a data flow diagram?

About 4,430,000 results (0.42 seconds)

A **data flow diagram** (**DFD**) is a graphical representation of the "**flow**" of **data** through an information system, modelling its process aspects. A **DFD** is often used as a preliminary step to create an overview of the system, which can later be elaborated.

Data flow diagram - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/**Data_flow_diagram** Wikipedia

infotex

Why?

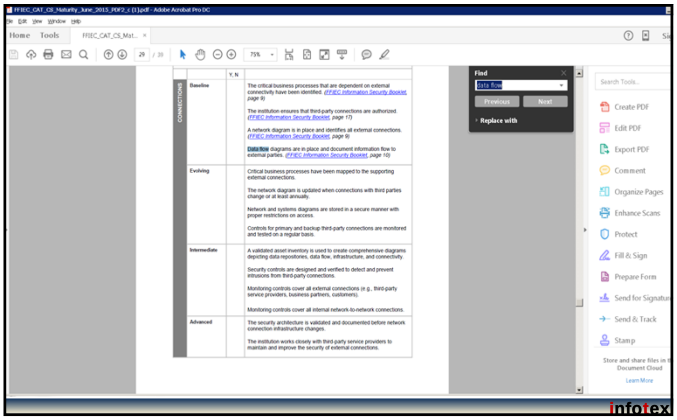
- Cybersecurity Assessment Tool

  "Nothing New"

  Seems to be true . . . .

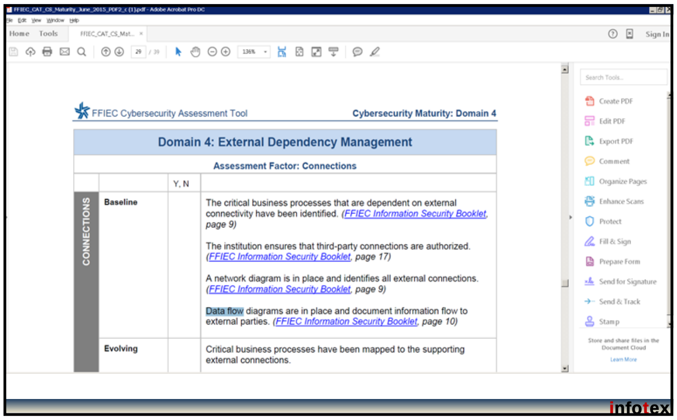
  . . . . but auditors were "scaling this one down."

infotex



		Y, N	
CONNECTIONS	**Baseline**		The critical business processes that are dependent on external connectivity have been identified. (*FFIEC Information Security Booklet, page 9*) The institution ensures that third-party connections are authorized. (*FFIEC Information Security Booklet, page 17*) A network diagram is in place and identifies all external connections. (*FFIEC Information Security Booklet, page 9*) Data flow diagrams are in place and document information flow to external parties. (*FFIEC Information Security Booklet, page 10*)
	Evolving		Critical business processes have been mapped to the supporting external connections. The network diagram is updated when connections with third parties change or at least annually. Network and systems diagrams are stored in a secure manner with proper restrictions on access. Controls for primary and backup third-party connections are monitored and tested on a regular basis.
	Intermediate		A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity. Security controls are designed and verified to detect and prevent intrusions from third-party connections. Monitoring controls cover all external connections (e.g., third-party service providers, business partners, customers). Monitoring controls cover all internal network-to-network connections.
	Advanced		The security architecture is validated and documented before network connection infrastructure changes. The institution works closely with third-party service providers to maintain and improve the security of external connections.

infotex

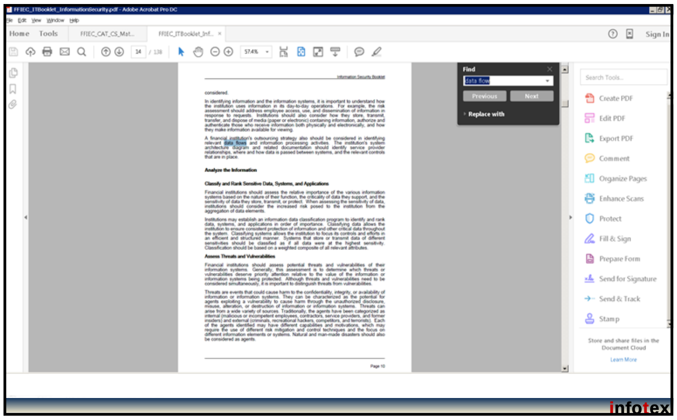


FFIEC Cybersecurity Assessment Tool — Cybersecurity Maturity: Domain 4

Domain 4: External Dependency Management

Assessment Factor: Connections

		Y, N	
CONNECTIONS	Baseline		The critical business processes that are dependent on external connectivity have been identified. (*FFIEC Information Security Booklet, page 9*) The institution ensures that third-party connections are authorized. (*FFIEC Information Security Booklet, page 17*) A network diagram is in place and identifies all external connections. (*FFIEC Information Security Booklet, page 9*) Data flow diagrams are in place and document information flow to external parties. (*FFIEC Information Security Booklet, page 10*)
	Evolving		Critical business processes have been mapped to the supporting external connections.



Information Security Booklet

considered.

In identifying information and the information systems, it is important to understand how the institution uses information in its day-to-day operations. For example, the risk assessment should address employee access, use, and dissemination of information in response to requests. Institutions should also consider how they store, transmit, transfer, and dispose of media (paper or electronic) containing information, authorize and authenticate those who receive information both physically and electronically, and how they make information available for viewing.

A financial institution's outsourcing strategy also should be considered in identifying relevant data flows and information processing activities. The institution's system architecture diagram and related documentation should identify service provider relationships, where and how data is passed between systems, and the relevant controls that are in place.

Analyze the Information

Classify and Rank Sensitive Data, Systems, and Applications

Financial institutions should assess the relative importance of the various information systems based on the nature of their function, the criticality of data they support, and the sensitivity of data they store, transmit, or protect. When assessing the sensitivity of data, institutions should consider the increased risk posed to the institution from the aggregation of data elements.

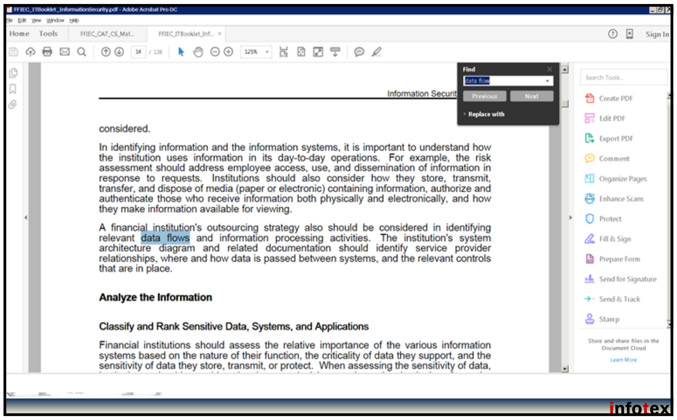
Institutions may establish an information data classification program to identify and rank data, systems, and applications in order of importance. Classifying data allows the institution to ensure consistent protection of information and other critical data throughout the system. Classifying systems allows the institution to focus its controls and efforts in an efficient and structured manner. Systems that store or transmit data of different sensitivities should be classified as if all data were at the highest sensitivity. Classification should be based on a weighted composite of all relevant attributes.

Assess Threats and Vulnerabilities

Financial institutions should assess potential threats and vulnerabilities of their information systems. Generally, this assessment is to determine which threats or vulnerabilities deserve priority attention relative to the value of the information or information systems being protected. Although threats and vulnerabilities need to be considered simultaneously, it is important to distinguish threats from vulnerabilities.

Threats are events that could cause harm to the confidentiality, integrity, or availability of information or information systems. They can be characterized as the potential for agents exploiting a vulnerability to cause harm through the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Threats can arise from a wide variety of sources. Traditionally, the agents have been categorized as internal (malicious or incompetent employees, contractors, service providers, and former insiders) and external (criminals, recreational hackers, competitors, and terrorists). Each of the agents identified may have different capabilities and motivations, which may require the use of different risk mitigation and control techniques and the focus on different information elements or systems. Natural and man-made disasters should also be considered as agents.

Page 10



Information Securit

considered.

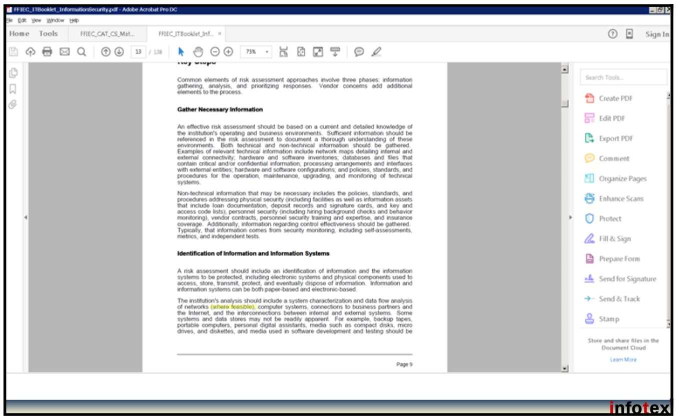
In identifying information and the information systems, it is important to understand how the institution uses information in its day-to-day operations. For example, the risk assessment should address employee access, use, and dissemination of information in response to requests. Institutions should also consider how they store, transmit, transfer, and dispose of media (paper or electronic) containing information, authorize and authenticate those who receive information both physically and electronically, and how they make information available for viewing.

A financial institution's outsourcing strategy also should be considered in identifying relevant data flows and information processing activities. The institution's system architecture diagram and related documentation should identify service provider relationships, where and how data is passed between systems, and the relevant controls that are in place.

Analyze the Information

Classify and Rank Sensitive Data, Systems, and Applications

Financial institutions should assess the relative importance of the various information systems based on the nature of their function, the criticality of data they support, and the sensitivity of data they store, transmit, or protect. When assessing the sensitivity of data,


FFIEC_ITBooklet_InformationSecurity.pdf - Adobe Acrobat Pro DC
File Edit View Window Help
Home Tools FFIEC_CAT_CS_Mat... FFIEC_ITBooklet_Inf... ×
Sign In
13 / 138
75%
Search Tools...
Create PDF
Edit PDF
Export PDF
Comment
Organize Pages
Enhance Scans
Protect
Fill & Sign
Prepare Form
Send for Signature
Send & Track
Stamp
Store and share files in the Document Cloud
Learn More
infotex

Key Steps

Common elements of risk assessment approaches involve three phases: information gathering, analysis, and prioritizing responses. Vendor concerns add additional elements to the process.

Gather Necessary Information

An effective risk assessment should be based on a current and detailed knowledge of the institution's operating and business environments. Sufficient information should be referenced in the risk assessment to document a thorough understanding of these environments. Both technical and non-technical information should be gathered. Examples of relevant technical information include network maps detailing internal and external connectivity; hardware and software inventories; databases and files that contain critical and/or confidential information; processing arrangements and interfaces with external entities; hardware and software configurations; and policies, standards, and procedures for the operation, maintenance, upgrading, and monitoring of technical systems.

Non-technical information that may be necessary includes the policies, standards, and procedures addressing physical security (including facilities as well as information assets that include loan documentation, deposit records and signature cards, and key and access code lists), personnel security (including hiring background checks and behavior monitoring), vendor contracts, personnel security training and expertise, and insurance coverage. Additionally, information regarding control effectiveness should be gathered. Typically, that information comes from security monitoring, including self-assessments, metrics, and independent tests.

Identification of Information and Information Systems

A risk assessment should include an identification of information and the information systems to be protected, including electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information and information systems can be both paper-based and electronic-based.

The institution's analysis should include a system characterization and data flow analysis of networks (where feasible), computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems. Some systems and data stores may not be readily apparent. For example, backup tapes, portable computers, personal digital assistants, media such as compact disks, micro drives, and diskettes, and media used in software development and testing should be

Page 9

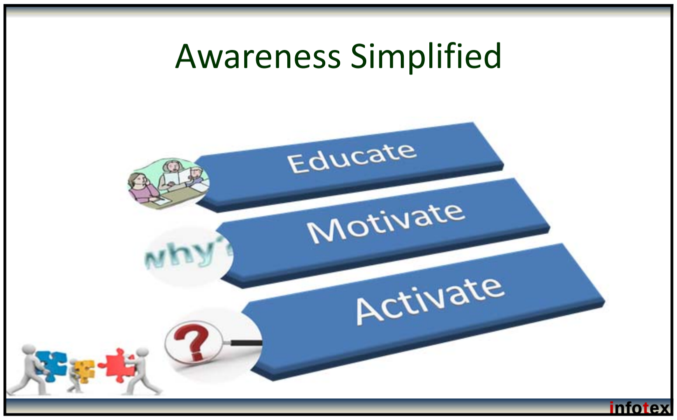
And yet . . . .

- We want to claim we're at baseline . . .
- It takes maybe 15-20 minutes per diagram . . .
- We CAN gain value from the process!

Who

- If we use the diagramming process as an Awareness Training Process.

Awareness in All Directions
Board
Management
Vendors
Technical
User
Customers



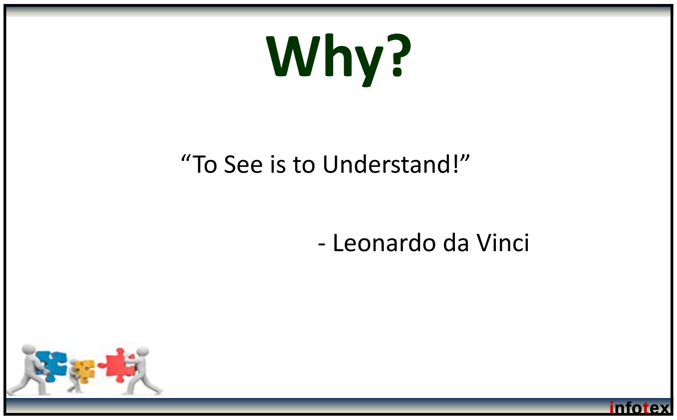
Awareness Simplified

Educate

Motivate

Activate

infotex

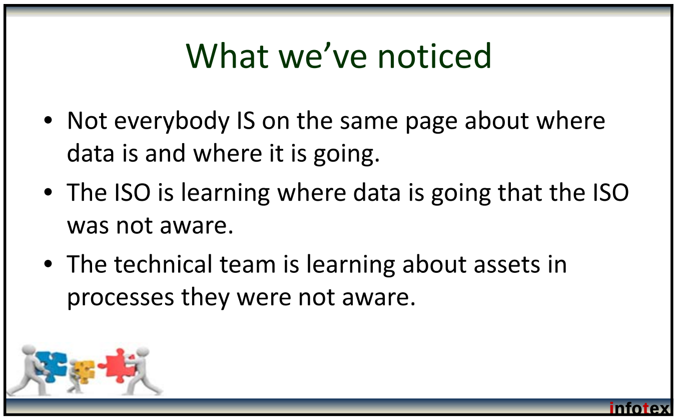


Why?

"To See is to Understand!"

- Leonardo da Vinci

infotex



What we've noticed

- Not everybody IS on the same page about where data is and where it is going.
- The ISO is learning where data is going that the ISO was not aware.
- The technical team is learning about assets in processes they were not aware.

infotex

What we suspect

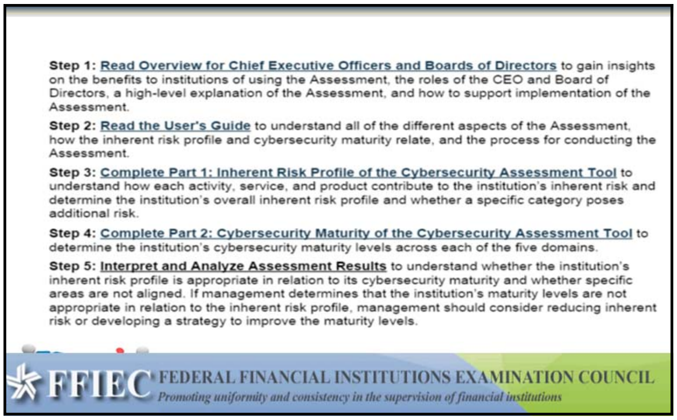
- You will get more value out of the process SHOWING THE DIAGRAM than drawing it.
- Before showing the diagram to management, your team members may want to review it!

infotex

When?

- Where are you in your five step process?

infotex



Step 1: Read Overview for Chief Executive Officers and Boards of Directors to gain insights on the benefits to institutions of using the Assessment, the roles of the CEO and Board of Directors, a high-level explanation of the Assessment, and how to support implementation of the Assessment.

Step 2: Read the User's Guide to understand all of the different aspects of the Assessment, how the inherent risk profile and cybersecurity maturity relate, and the process for conducting the Assessment.

Step 3: Complete Part 1: Inherent Risk Profile of the Cybersecurity Assessment Tool to understand how each activity, service, and product contribute to the institution's inherent risk and determine the institution's overall inherent risk profile and whether a specific category poses additional risk.

Step 4: Complete Part 2: Cybersecurity Maturity of the Cybersecurity Assessment Tool to determine the institution's cybersecurity maturity levels across each of the five domains.

Step 5: Interpret and Analyze Assessment Results to understand whether the institution's inherent risk profile is appropriate in relation to its cybersecurity maturity and whether specific areas are not aligned. If management determines that the institution's maturity levels are not appropriate in relation to the inherent risk profile, management should consider reducing inherent risk or developing a strategy to improve the maturity levels.

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

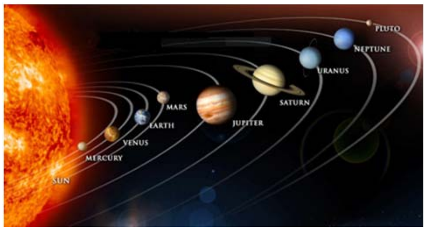
Summary

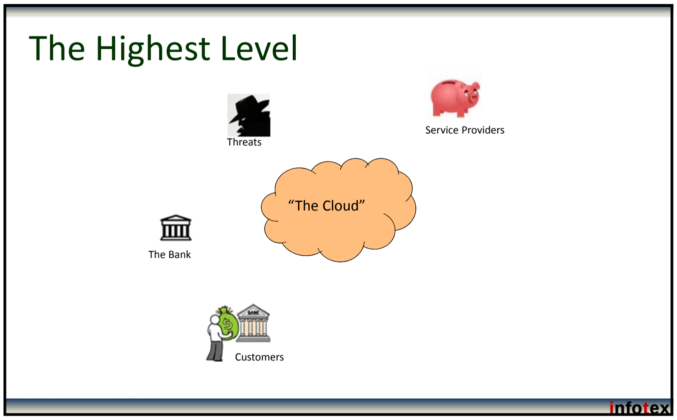
- A data flow diagram should show where data leaves your control into the "outsourcing realm."
- Work in iterations: Data Flow Diagramming should be seen as an awareness exercise to be conducted during mitigation of CAT identified cyber-risk.
- By seeing data flow, our new awareness motivates us to protect that data, and activates awareness.

Agenda

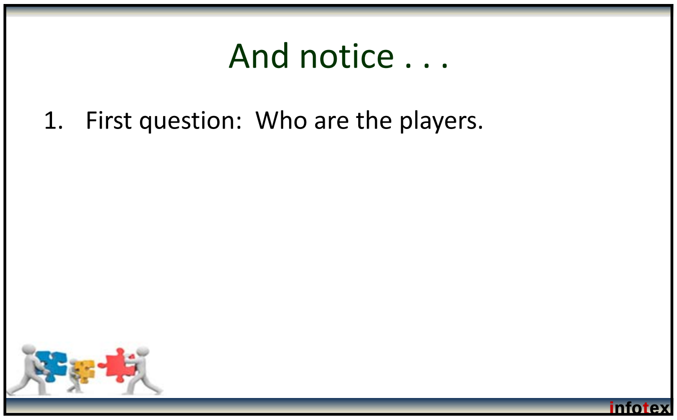
- Overview: What and Why? When?
- Who: If we have to, let's get some value!
- How
  - Expectations, Standards, Conventions
  - Tools, Resources, Starting Points
  - Five Question Process

Not who, scale!



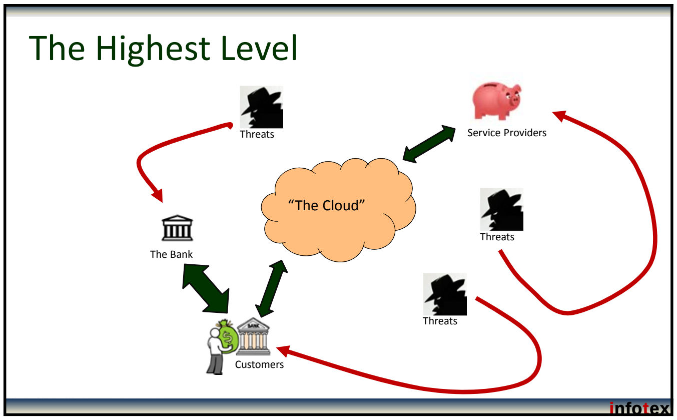


The Highest Level

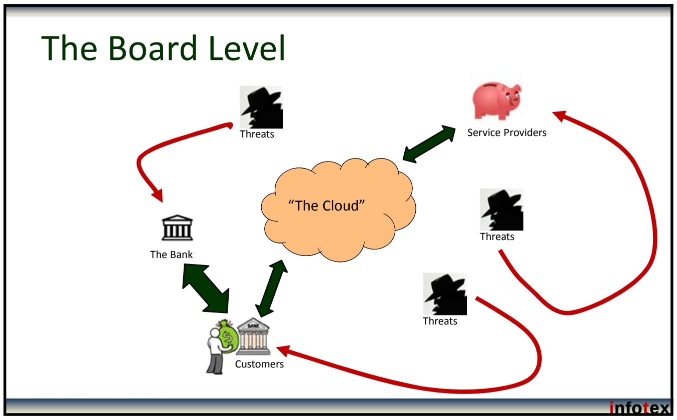


And notice . . .

1. First question: Who are the players.



The Highest Level



The Board Level

Threats

Service Providers

"The Cloud"

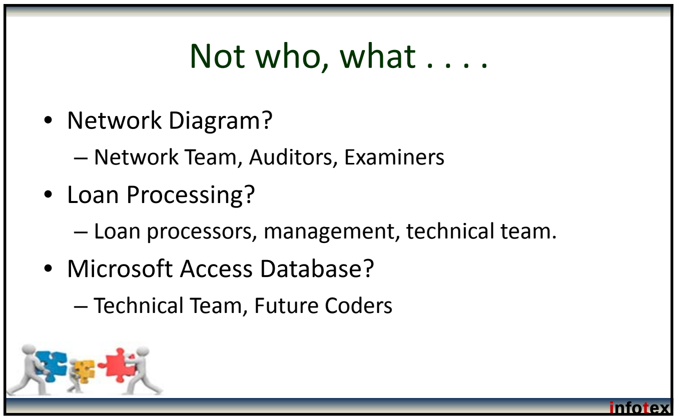
The Bank

Threats

Threats

Customers

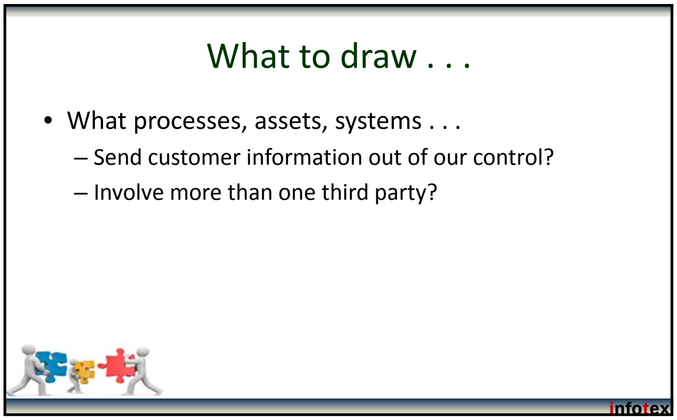
infotex



Not who, what . . . .

- Network Diagram?
  - Network Team, Auditors, Examiners
- Loan Processing?
  - Loan processors, management, technical team.
- Microsoft Access Database?
  - Technical Team, Future Coders

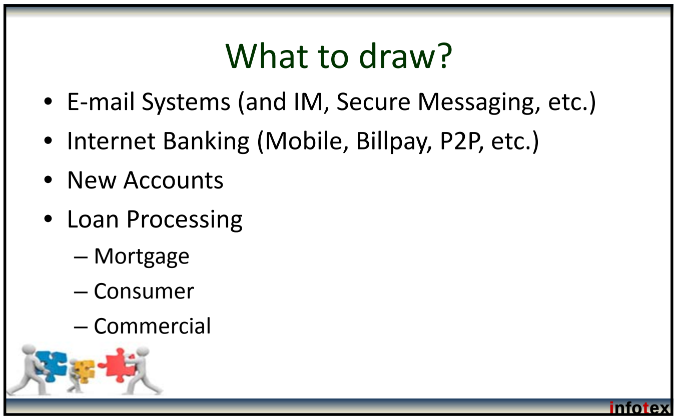
infotex



What to draw . . .

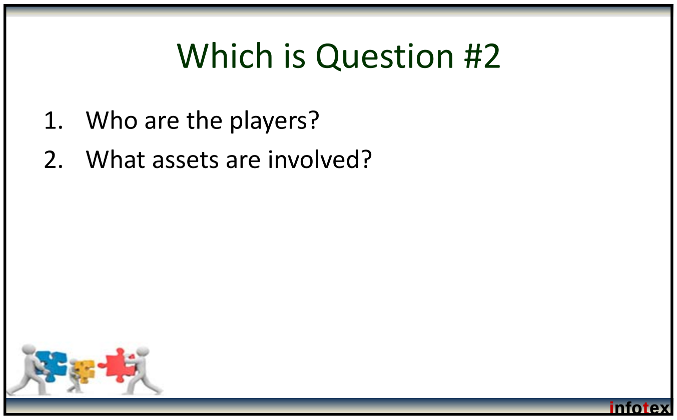
- What processes, assets, systems . . .
  - Send customer information out of our control?
  - Involve more than one third party?

infotex



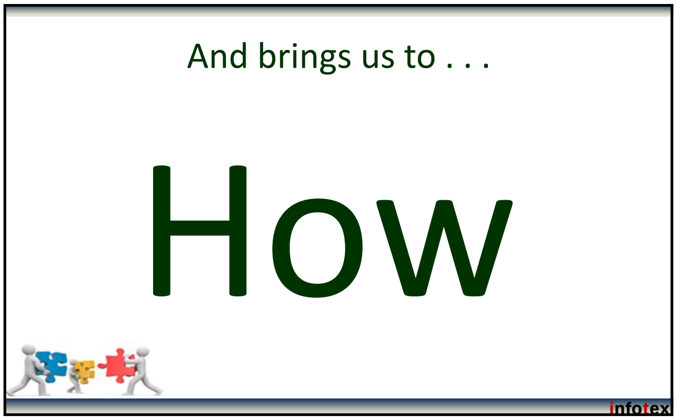
What to draw?

- E-mail Systems (and IM, Secure Messaging, etc.)
- Internet Banking (Mobile, Billpay, P2P, etc.)
- New Accounts
- Loan Processing
  - Mortgage
  - Consumer
  - Commercial



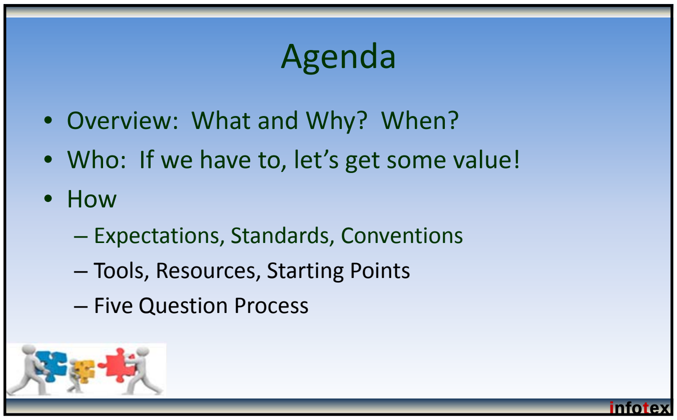
Which is Question #2

1. Who are the players?
2. What assets are involved?



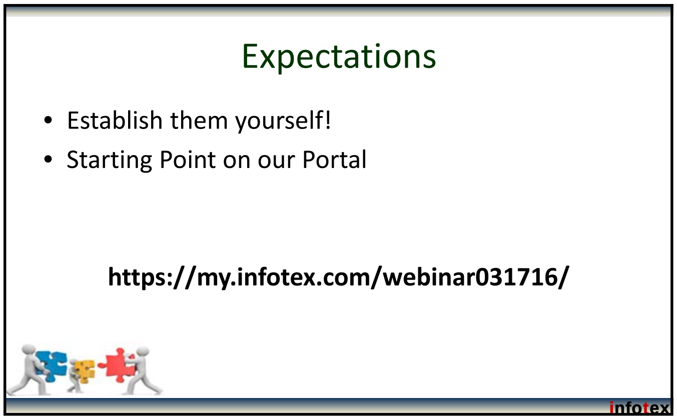
And brings us to . . .

How



Agenda

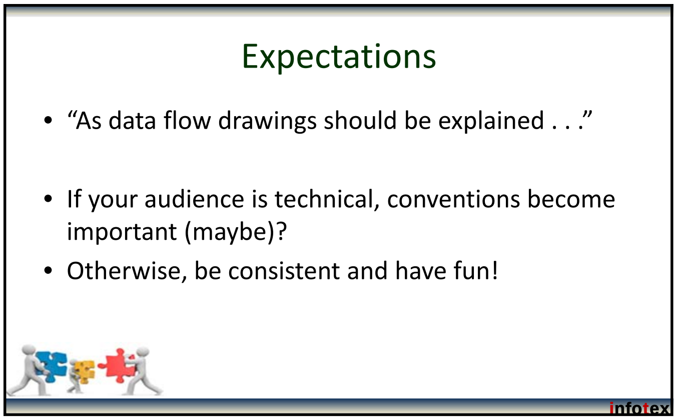
- Overview: What and Why? When?
- Who: If we have to, let’s get some value!
- How
  - Expectations, Standards, Conventions
  - Tools, Resources, Starting Points
  - Five Question Process



Expectations

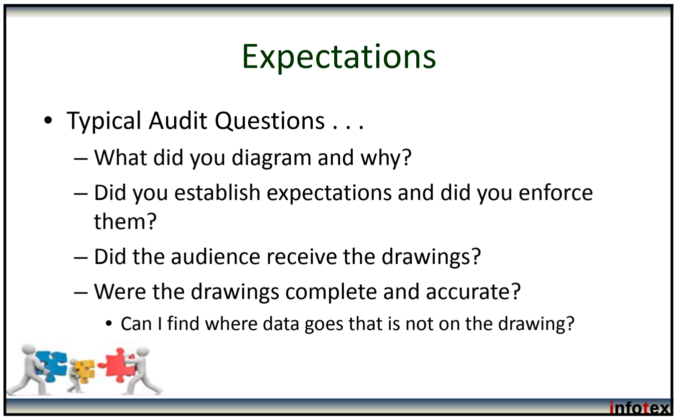
- Establish them yourself!
- Starting Point on our Portal

https://my.infotex.com/webinar031716/



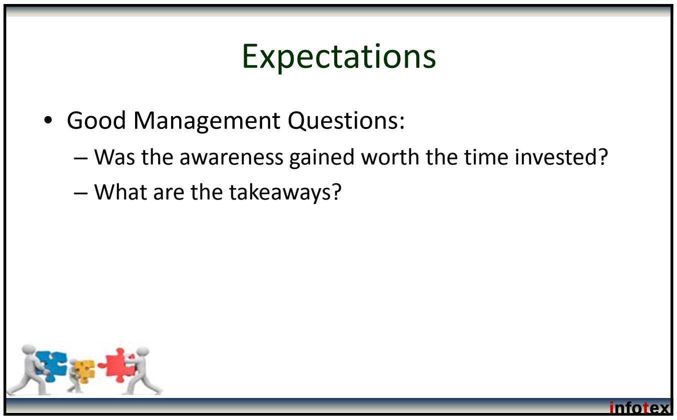
Expectations

- “As data flow drawings should be explained . . .”
- If your audience is technical, conventions become important (maybe)?
- Otherwise, be consistent and have fun!



Expectations

- Typical Audit Questions . . .
  - What did you diagram and why?
  - Did you establish expectations and did you enforce them?
  - Did the audience receive the drawings?
  - Were the drawings complete and accurate?
    - Can I find where data goes that is not on the drawing?

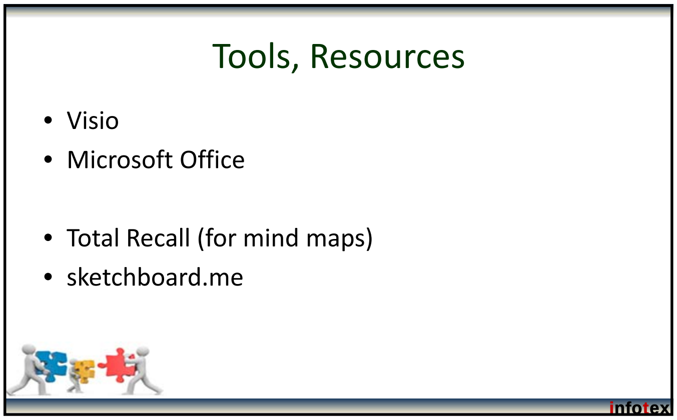


Expectations

- Good Management Questions:
  - Was the awareness gained worth the time invested?
  - What are the takeaways?

Agenda

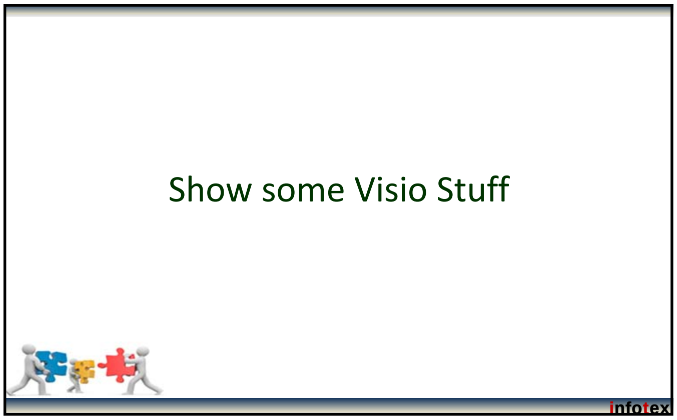
- Overview: What and Why? When?
- Who: If we have to, let's get some value!
- How
  - Expectations, Standards, Conventions
  - Tools, Resources, Starting Points
  - Five Question Process



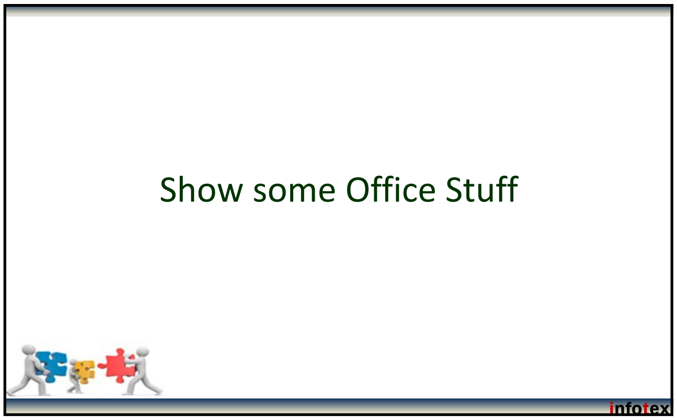
Tools, Resources

- Visio
- Microsoft Office

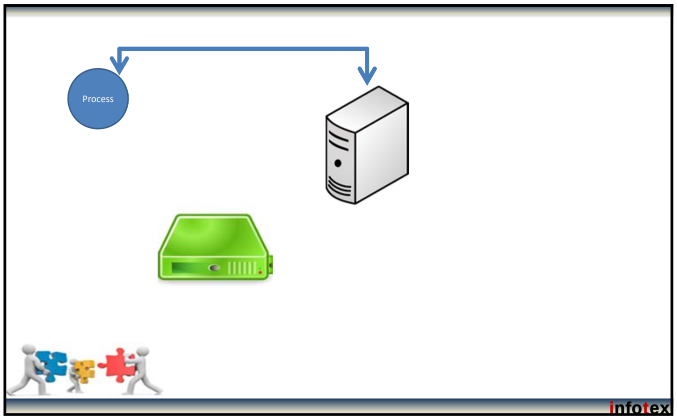
- Total Recall (for mind maps)
- sketchboard.me



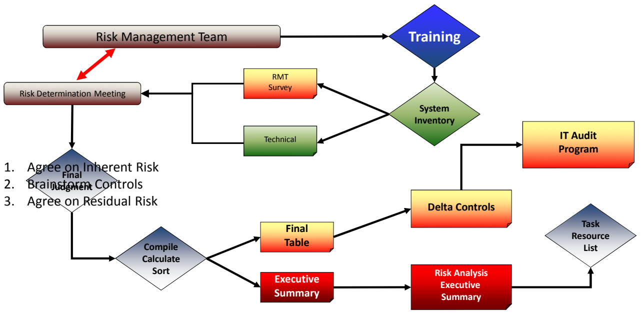
Show some Visio Stuff



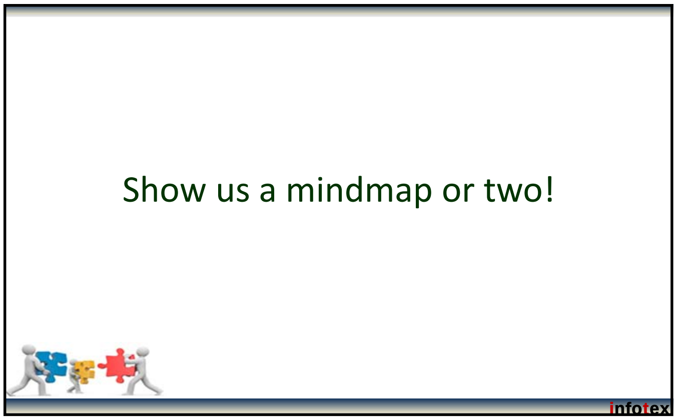
Show some Office Stuff



IT Risk Analysis Process



1. Agree on Inherent Risk
2. Brainstorm Controls
3. Agree on Residual Risk


Show us a mindmap or two!

Example of Mind Map

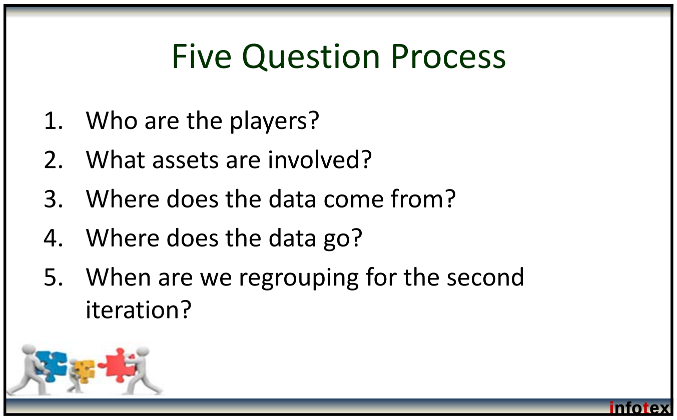
- http://my.infotex.com/alarming-recurring-finding/

Starting Points on sketchboard.me

my.infotex.com/dfds

Agenda

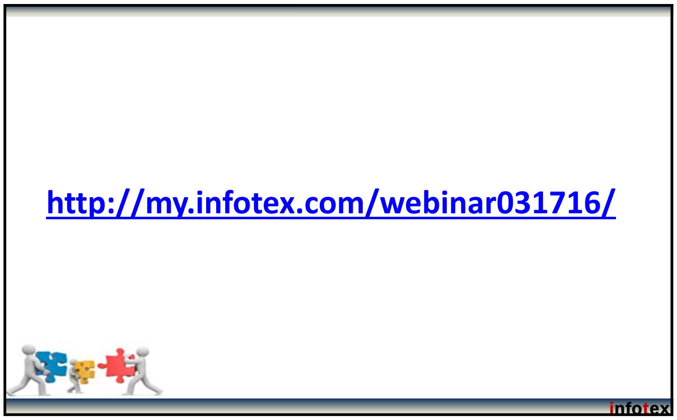
- Overview: What and Why? When?
- Who: If we have to, let's get some value!
- How
  - Expectations, Standards, Conventions
  - Tools, Resources, Starting Points
  - Five Question Process



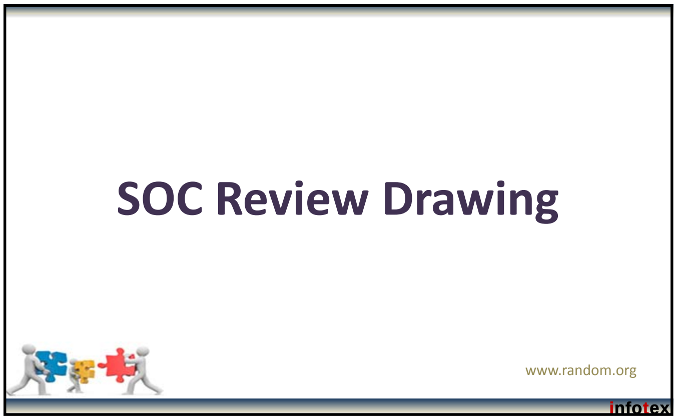
Five Question Process

1. Who are the players?
2. What assets are involved?
3. Where does the data come from?
4. Where does the data go?
5. When are we regrouping for the second iteration?

?



http://my.infotex.com/webinar031716/



SOC Review Drawing

www.random.org

infotex

Thank you!

infotex

Thank you!

infotex