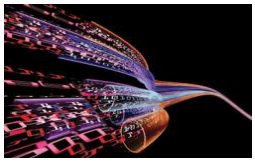
® v1.0



Overview

This platform will give the subscriber (or any company offering services) the ability to visually represent the flow of information at each step of the service. Subscribers to this platform should be able to sign up by creating an account. I, as the platform owner will be the master administrator for the entire platform regardless of how many users subscribe. At the master administration level, I will need the ability to add other master administrators. The subscriber will be the owner/administrator for their service. At this level, once an account has been created they should be able to define a service. The definition will include the description of service. The subscriber will be able indicate the regulations or governing standards, internal data classification and there will be an area where the subscriber can upload documents of their choosing. Once complete, the subscriber can began building the information and process flow of the service. The service flow diagram will be similar to a data flow diagram but with more functionality. The subscriber will start with a icon on a blank canvas (web page). The subscriber should be able to click on that icon and be presented with form that allows them to input information. See **Service/process step Functionality** section below for the contents of the form. Once they have defined the step, the subscriber should be able to place an arrow to the next step. They should be able to repeat this until the entire service has been mapped out. Once the service has been mapped out the subscriber should provide a name and version of the service and save it. The subscriber can then email a link to the service flow diagram to the new user. The email form should contain the name and email address of the intended recipient. The email recipient should be able to click the link and be re-directed to the site. Once on the site, the email recipient should be able to create an account. After this is done, the email recipient should be able to see all of the services being shared with them.

Global Functionality

- **Plain text comment field**
    - Overall service description

- **Text box comment field 1**
    - Regulations/Legal statues (i.e. GLBA, GDPR)
    - Governing Standard (i.e. PCI)
- **Drop down menu – Internal data classification**
    - Public
    - Confidential
    - Restricted
    - Highly Restricted
- Input 'Global controls' for People, Processes & Technology
- **Document repository**
    - Only service provider can upload documents
    -
- Customer icons – Each icon represents a phase or step in the service
- **Email functionality**
    - Service provider can 'share' service flow with client by emailing a link to service flow
    - Service provider can select access level for clients (read, write, etc)
    - Service provider can determine how long service flow is shared with client
    - Platform should give service provider the ability to notify customers via email of any updates to flow diagram or new document uploads.
- **Reporting functionality**
    - Summary of overall service description
    - Regulations and governing standards
    - Data fields per each step in the service

Service/process step Functionality

- Icon is a hyperlink that opens a form with the fields below:
- Step description
- Info Sent: Data fields [Required Y/N?]
    - Sending party
- Transport medium
    - Transport protocol
- Encryption type
- Potential vulnerabilities & threats
- Input 'Phase specific' controls for People, Processes & Technology
- Upload 'phase specific' documents
- Comments

Example Service Information Flow: Online Order

Object: Customer
Step Desc: Customer calls Acme to order new tires for her/his car
Data: Name, Address, Email, Phone, CC#, Vehicle make/model/year
Data Xfer Medium: Phone

Security Controls: None
Documents: None
Comments: No controls at this stage as the process is initiated by the customer

Object: Customer Service Rep
Step Desc: Takes customer order via telephone
Data: Name, Address, Email, Phone, CC#, Vehicle make/model/year
Data Xfer Medium: Phone, Acme Ordering application
Security Controls: Background checks, IT Security Awareness training
Documents: HR Policy
Comments: CSR receives job training and yearly information security training

Object: Third Party Datacenter
Step Desc: Acme Production Environment
Data: Name, Address, Email, Phone, CC#, Vehicle make/model/year
Data Xfer Medium: Encrypted direct connection
Security Controls: 3rd Party risk assessment, locked cages, CCTV, Redundant power
Documents: SOC 2 Type 2, Acme Physical security policy
Comments: Acme conducts yearly reviews of data center. Acme physical security policy details physical security requirements.

Object: Acme Ordering application
Step Desc: CSR enters details of customer orders
Data: Name, Address, Email, Phone, CC#, Vehicle make/model/year, Order comments
Data Xfer Medium: Internal datacenter network,
Security Controls: Secure coding, vulnerability/pen tests, encryption, DLP
Documents: SDLC Policy, Access control policy, Network Security Policy
Comments: Order is sent to warehouse for fulfillment

Administrative Functionality

- **Platform owner/master administrator**
  - Change own password
  - Create other platform administrators
  - Run report for number of users and number of services per user for entire platform
  - Disable service owner/administrator accounts
  - Disable services created by service owner
- **Service owner/administrator**
  - Change own password
  - Create other service administrators
  - Add/change/delete new services
  - Notify end customer of service change or document upload via email
  - Share service flow via email
  - Determine access level when sharing
  - Disable service administrator accounts
  - Run report for number of services they own
    - Report will contain number of user accounts that have share access to the service flow and level of access per user account
  - Revoke access to service (based on email address)

Example Customer Icon Library: