ControlCase
Compliance as a Service

EU'S General Data Protection Regulation

Afy Merchant

ControlCase Annual Conference – Miami, Florida USA 2017

Agenda

- ✓ What is GDPR ?
- ✓ What does GDPR mean for you
- ✓ GDPR Immediate Next Steps
- ✓ GDPR Tactical Compliance
- ✓ ControlCase GDPR solutions
- ✓ Panel discussions

ControlCase
Compliance as a Service

What is GDPR?

ControlCase
Compliance as a Service

What is General Data Protection Regulation (GDPR)?

GDPR

Related to processing of personal data

Harmonizes data privacy laws/regulation across Europe

Protects EU citizen data privacy

Established fines for non compliance

Establishes breach notification guidelines

Goes into effect May 2018

Types of data include address, phone numbers, email address, name, Biometric information

ControlCase
Compliance as a Service

Key Definitions

Data Processor vs Data Controller

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

Regulation vs Directive

A regulation is a binding legislative act. It must be applied in its entirety across the EU, while a directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how. It is important to note that the GDPR is a regulation, in contrast the previous legislation, which is a directive.

DPA

Data Protection Authority

What does GDPR mean for you?

ControlCase
Compliance as a Service

What is General Data Protection Regulation (GDPR)?

GDPR

- Large Sanctions
- Impacts Everyone
- Effective Data Protection
- Compulsory reporting of breaches
- Data Processing Permission
- Expanded definition of personal data
- Right to be forgotten
- Dedicated "Data Protection Officer"
- Privacy by Design

GDPR – What it means for you

Large Sanctions –Fines for not complying with GDPR can go up to 20 million euros, or 4% of a company's overall income (depending on which value is higher).

Impacts Everyone —Each and every organization has to consistently protect personal data. You also have to protect employee personal data, customer information, patient databases, etc.

GDPR – What it means for you

Effective Data Protection —Your company has to be ready to prove that your technical and organizational measures for data protection function properly.

Compulsory Reporting of breaches —The Data Protection Authority must be notified within 72 hours of breach discovery.

ControlCase
Compliance as a Service

GDPR – What it means for you

Data Processing Permission –Free and clear authorization is required. Requests for approval must be simple and easy to understand.

Expanded definition of personnel data — Personal data also includes email addresses, IP addresses, cookies, and genetic and biometric information.

GDPR – What it means for you

Right to be forgotten –Each person has the right to require that you delete his/her personal information without delay.

Dedicated "Data Protection Officer" — Organizations systematically processing personal data are required to have a person appointed to the role of "Data Protection Officer“

ControlCase
Compliance as a Service

GDPR – What it means for you

Privacy by Design –Personal data protection must be implemented in the design stage of a security measure.

ControlCase
Compliance as a Service

GDPR Immediate Next Steps

GDPR: Immediate Next Steps - Data Impact Assessment

- ✓ Must Carry out **Data** Identification **and Impact Assessment (DIA)** as determined by supervisory authorities
- ✓ It should be managed by **Data Protection Officer (DPO)**
- ✓ Assessment Must Include:
  - ▪ Details of processing operations
  - ▪ Purpose of processing
  - ▪ Risks to privacy of individuals
  - ▪ Security assessment
- ✓ When
  - ▪ Prior to “processing” personal data
  - ▪ After any changes to systems or processing mechanism

GDPR: Immediate Next Steps - Data Impact Assessment

- ✓ Data Protection Officer is required in multiple scenarios including:
  - ▪ Processing by public bodies
  - ▪ Processor includes storage/process/transmission of large amounts of personal information
- ✓ Multiple entities can combine to have a single DPO and can be an employee or outsourced
- ✓ Must be independent and “cannot” be dismissed for doing their job
- ✓ Tasks include
  - ▪ Monitor compliance to GDPR
  - ▪ Provide advice within the organization for GDPR
  - ▪ Coordinate with supervisory authority/DPA

GDPR Tactical Next Steps

ControlCase

Compliance as a Service

GDPR: Immediate Next Steps - Data Impact Assessment

- ✓ Principles relating to processing of personal data
- ✓ Rights of individuals
- ✓ Consent
- ✓ Responsibility of the controller/processor
- ✓ Security of data
- ✓ Data processing impact assessment
- ✓ Data protection officer

ControlCase
Compliance as a Service

GDPR – What it means for you

Security of Processing

Asset & Vulnerability Management
Data Management
Logical Access
Physical Access
Risk Assessment
Policy Management
Third Party Management

Right Management

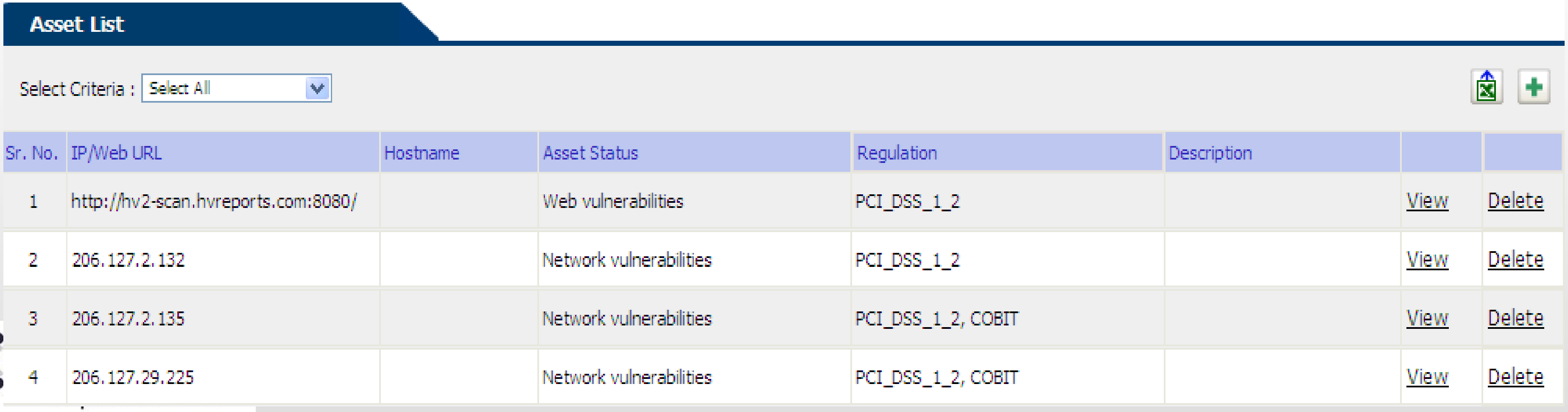
Breach Notification Management

Privacy Management

ControlCase
Compliance as a Service

Asset and Vulnerability Management

- ✓ Asset list
- ✓ Management of vulnerabilities and dispositions
- ✓ Training to development and support staff
- ✓ Management reporting if unmitigated vulnerability



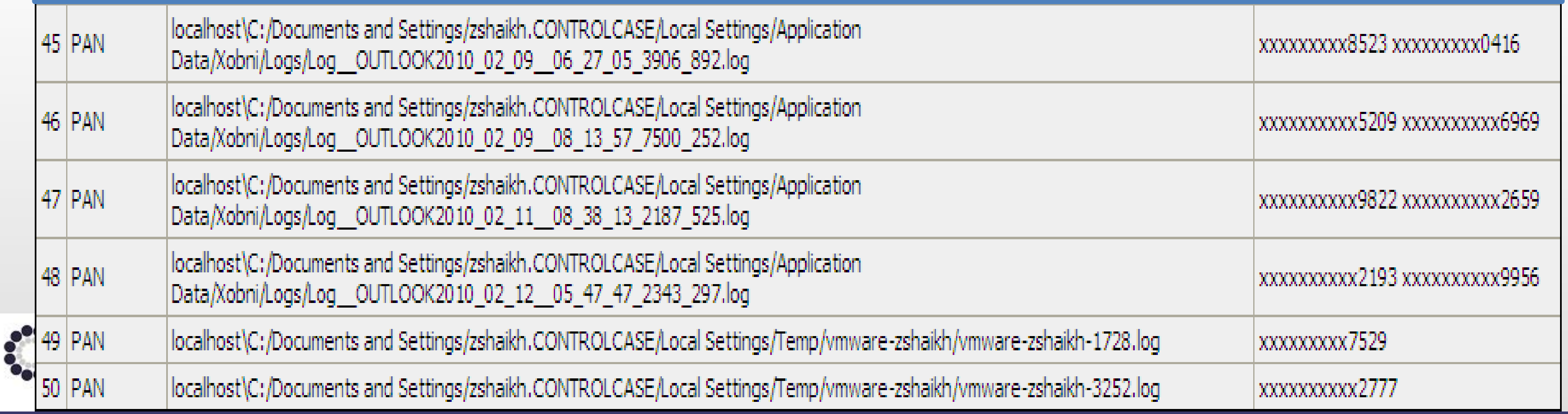
Asset List

Select Criteria : Select All

Sr. No.	IP/Web URL	Hostname	Asset Status	Regulation	Description		
1	http://hv2-scan.hvreports.com:8080/		Web vulnerabilities	PCI_DSS_1_2		View	Delete
2	206.127.2.132		Network vulnerabilities	PCI_DSS_1_2		View	Delete
3	206.127.2.135		Network vulnerabilities	PCI_DSS_1_2, COBIT		View	Delete
4	206.127.29.225		Network vulnerabilities	PCI_DSS_1_2, COBIT		View	Delete

Data Management

- ✓ Identification of personally identifiable data
- ✓ Classification of data
- ✓ Encryption of data
- ✓ Monitoring of data



45	PAN	localhost\C:/Documents and Settings/zshaikh.CONTROLCASE/Local Settings/Application Data/Xobni/Logs/Log__OUTLOOK2010_02_09__06_27_05_3906_892.log	xxxxxxxxx8523 xxxxxxxxx0416
46	PAN	localhost\C:/Documents and Settings/zshaikh.CONTROLCASE/Local Settings/Application Data/Xobni/Logs/Log__OUTLOOK2010_02_09__08_13_57_7500_252.log	xxxxxxxxxx5209 xxxxxxxxxx6969
47	PAN	localhost\C:/Documents and Settings/zshaikh.CONTROLCASE/Local Settings/Application Data/Xobni/Logs/Log__OUTLOOK2010_02_11__08_38_13_2187_525.log	xxxxxxxxxx9822 xxxxxxxxxx2659
48	PAN	localhost\C:/Documents and Settings/zshaikh.CONTROLCASE/Local Settings/Application Data/Xobni/Logs/Log__OUTLOOK2010_02_12__05_47_47_2343_297.log	xxxxxxxxxx2193 xxxxxxxxxx9956
49	PAN	localhost\C:/Documents and Settings/zshaikh.CONTROLCASE/Local Settings/Temp/vmware-zshaikh/vmware-zshaikh-1728.log	xxxxxxxxx7529
50	PAN	localhost\C:/Documents and Settings/zshaikh.CONTROLCASE/Local Settings/Temp/vmware-zshaikh/vmware-zshaikh-3252.log	xxxxxxxxxx2777

Logical Access

- ✓ Username
- ✓ Password
- ✓ Access based on need to know
- ✓ Protection of data

ControlCase
Compliance as a Service

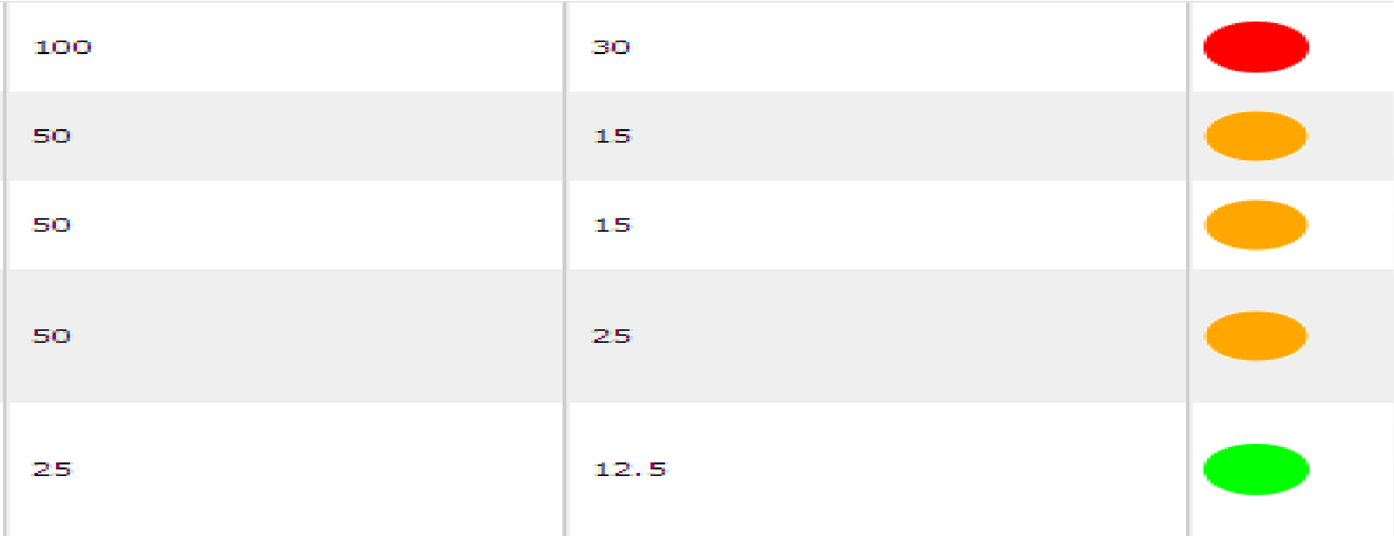
Physical Security

- ✓ Badges
- ✓ Visitor Access
- ✓ CCTV
- ✓ Biometric
- ✓ Media Inventory
- ✓ Media Destruction

ControlCase
Compliance as a Service

Risk Management

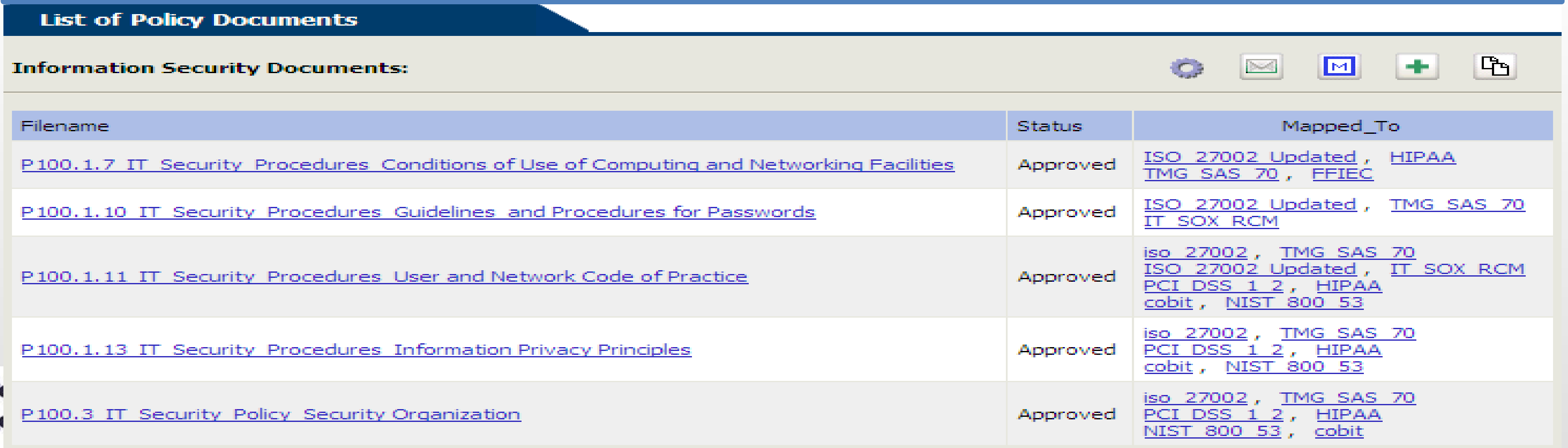
- ✓ Input of key criterion
- ✓ Numeric algorithms to compute risk
- ✓ Output of risk dashboards



100	30	🔴
50	15	🟠
50	15	🟠
50	25	🟠
25	12.5	🟢

Policy Management

- ✓ Appropriate update of policies and procedures
- ✓ Link/Mapping to controls and standards
- ✓ Communication, training and attestation
- ✓ Monitoring of compliance to corporate policies



List of Policy Documents

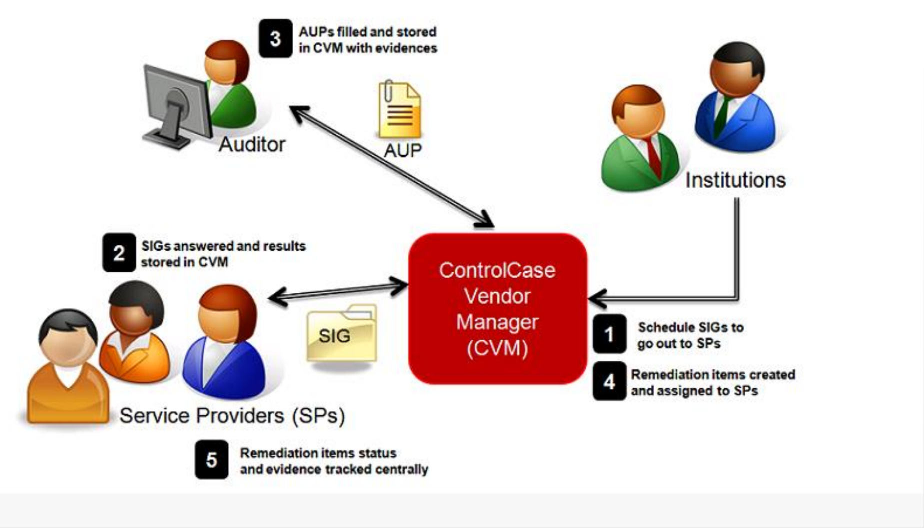
Information Security Documents:

Filename	Status	Mapped_To
P100.1.7 IT Security Procedures Conditions of Use of Computing and Networking Facilities	Approved	ISO 27002 Updated , HIPAA TMG SAS 70 , FFIEC
P100.1.10 IT Security Procedures Guidelines and Procedures for Passwords	Approved	ISO 27002 Updated , TMG SAS 70 IT SOX RCM
P100.1.11 IT Security Procedures User and Network Code of Practice	Approved	iso 27002 , TMG SAS 70 ISO 27002 Updated , IT SOX RCM PCI DSS 1 2 , HIPAA cobit , NIST 800 53
P100.1.13 IT Security Procedures Information Privacy Principles	Approved	iso 27002 , TMG SAS 70 PCI DSS 1 2 , HIPAA cobit , NIST 800 53
P100.3 IT Security Policy Security Organization	Approved	iso 27002 , TMG SAS 70 PCI DSS 1 2 , HIPAA NIST 800 53 , cobit

Vendor/Third Party Management

- ✓ Management of third parties/vendors
- ✓ Self attestation by third parties/vendors
- ✓ Remediation tracking

Reg/Standard	Coverage area
ISO 27001	A.6, A.10
PCI	12
EI3PA	12
HIPAA	164.308b1
FISMA	PS-3
FERC/NERC	Multiple Requirements



3 AUPs filled and stored in CVM with evidences

Auditor

AUP

Institutions

2 SIGs answered and results stored in CVM

ControlCase Vendor Manager (CVM)

SIG

1 Schedule SIGs to go out to SPs

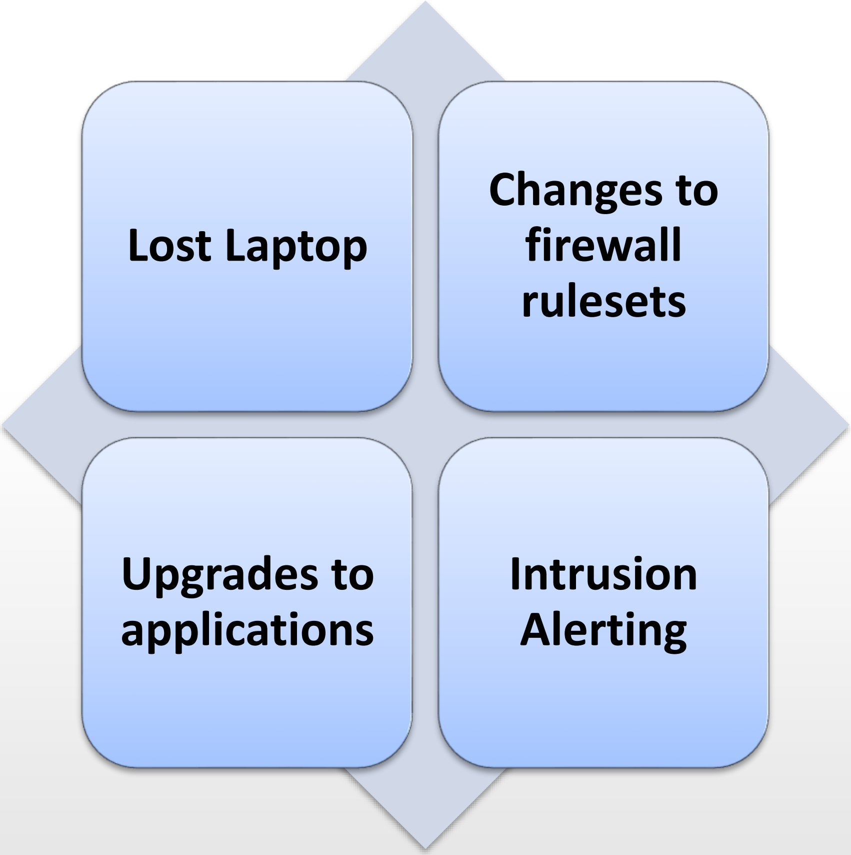
4 Remediation items created and assigned to SPs

Service Providers (SPs)

5 Remediation items status and evidence tracked centrally

Incident Management

- ✓ Monitoring
- ✓ Detection
- ✓ Reporting
- ✓ Responding
- ✓ Approving



ControlCase
Compliance as a Service

Rights Management

- ✓ **Rights of data subjects:**
  - Right to receive information on data processor
  - Right to ask for modification of data
  - Right to ask for deletion of data
  - Right to ask processor to restrict use of data for certain purposes
  - Right around movement of data
- ✓ **Processor Required to Provide These Details**
  - Requires breach notification to the Controlling Entity
  - Provides an accounting of disclosures.

Privacy Management

- ✓ **Privacy Rule Main Points:**
  - Requires appropriate safeguards to protect the privacy of personal information
  - Sets limits and conditions on the uses and disclosures that may be made of such information without authorization
  - Gives individuals rights over their health information, including rights to examine and obtain a copy of their records, and to request erasure or change
  - Records of processing activities
  - Right to "be forgotten"

- ✓ **For Third Parties**
  - Requires breach notification to the Controlling Entity
  - Provide an accounting of disclosures.

Breach Notification Management

- ✓ **Definition of Breach**
  - A breach is, generally, an impermissible use or disclosure that compromises the security or privacy of personal information.
- ✓ **Breach Notification Mechanism**
  - Notify to Data Protection Authorities (DPA) with 72 hours.
  - Notify individuals without undue delay.
  - Notify volume of breach.
  - Vendors/Third parties to notify the customer without undue delay.
- ✓ **Content of Breach Notification**
  - Approximate number of records compromised
  - Categories of data compromised
  - Point if contact of data protection officer
  - Likely consequences of data breach
  - Measures takes to address/mitigate the breach

ControlCase
Compliance as a Service

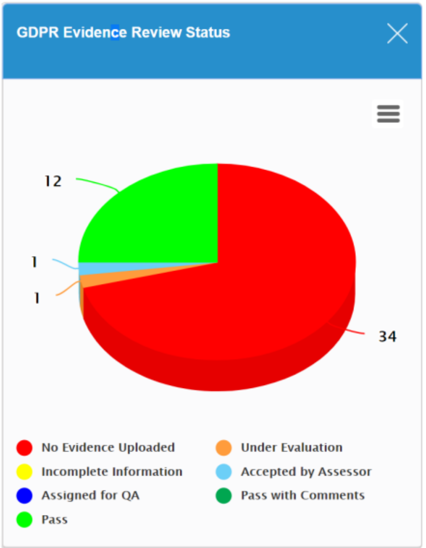
GDPR DIA Assessment

Data Impact Assessment

ControlCase
Compliance as a Service

ControlCase Solution 1: Data Impact Assessment

- ✓ 48 items in portal questionnaire
- ✓ 4 week engagement
- ✓ Assessment Includes
  - Review of processing operations documents
  - Risk assessment to privacy of individuals
  - Security assessment of personal data
- ✓ Deliverable
  - DIA Report (Required)
  - GDPR Certificate of Compliance (COC) if no gaps are foun
  - NOTE: Additional iterative review methodology can also be deployed until compliance is achieved
- ✓ Team
  - Security Assessor – Partnership Approach
  - Success Team: PMO Milestone Management & Account Manager for Escalation Management
- ✓ Secure Portal
  - Upload Evidence, See History of Comments & Track Status


GDPR Evidence Review Status
12
1
1
34
No Evidence Uploaded
Under Evaluation
Incomplete Information
Accepted by Assessor
Assigned for QA
Pass with Comments
Pass