AUTOMATED CYBER RISK OFFICER (ACRO) FOR GDPR

FOUR EASY STEPS TO HELP PREPARE YOUR ORAGNZIATION FOR GDPR

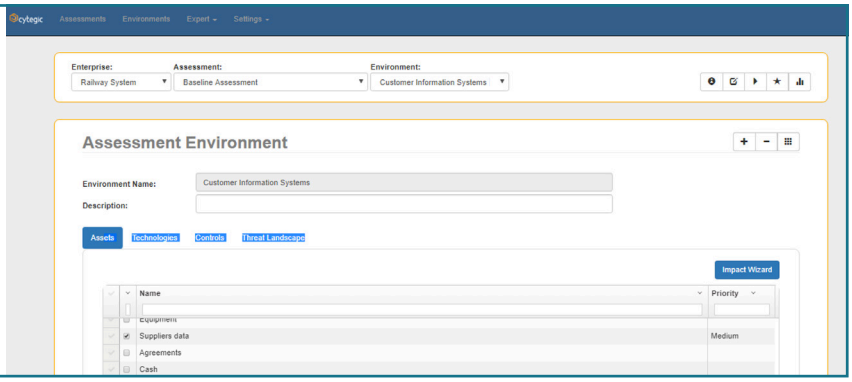
As a leading provider of cyber risk management solutions, Cytegic provides an automated end-to-end solution that encompasses the entire scope of cyber risk management.

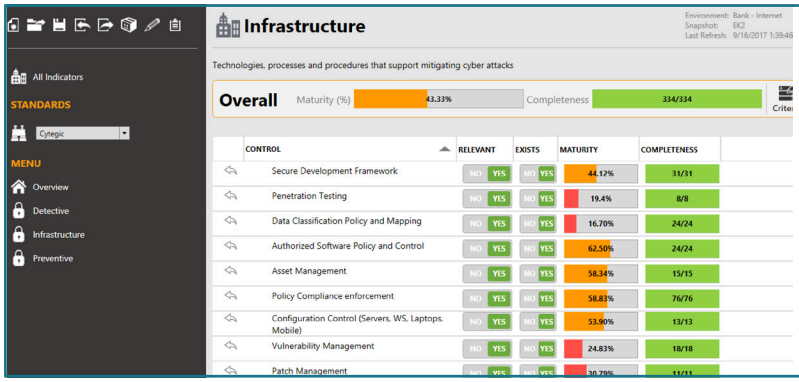
May 25th, 2018 marks the implementation date for the General Data Protection Regulation (GDPR) to go into effect. All organizations that hold EU customer data, even organziations outside of the EU must comply with the regulation as specified. With steep penalties segmented into two levels, organziations that fail to meet GDPR can and will face fines ranging from $10M+ for the first level and over $20M+ for the second level. As the implementation date approaches, it is mission-critical to conduct an assessment that provides your organization with a baseline on where you stand, and what needs to be accomplished to meet GDPR, while decreasing your overall cyber risk profile.

Cytegic has created a simple, four step intuitive assessment workflow that provides your organziation with GDPR specific reporting, dashboard and plan-of-action capability.

STEP 1:
ENVIRONEMNT SELECTION

Simply login to your Cytegic ACRO profile and select the environment and/or business unit you wish to assess for GDPR.





STEP 2:
DATA COLLECTION

Once your environment is selected, the data collection phase is required to assess the compliance level of the organization with GDPR requirements initiated.

cytegic

STEP 3:
ANALYTICS & REPORTING

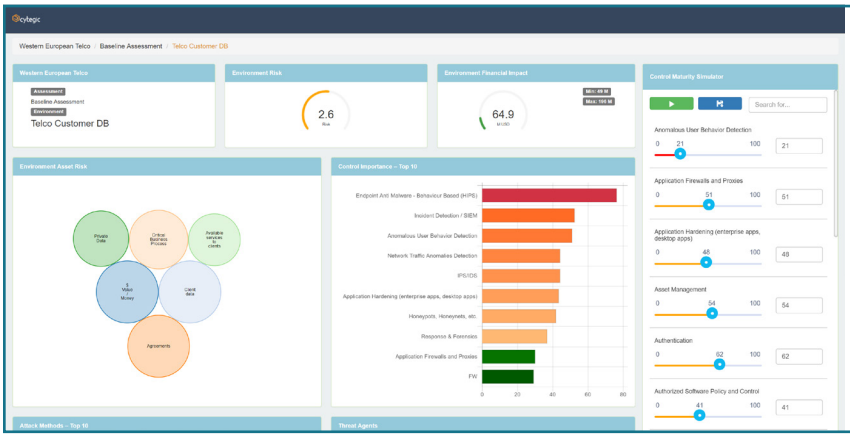
Once the system is populated with data, an analysis of your organizations compliance level with GDPR requirements can be performed.

When completed, you will be provided with a report that presents the difference between controls maturity as perceived by your organization, to the controls maturity derived from technical indicators of maturity gathered directly from the controls configuration files.

[[CompanyName]] GDPR compliance report

Detailed Findings

Section	Score
Chapter 1: General Provisions	**45**
Chapter 1: General Provisions	45
Article 3: Territorial scope	40
Has the organization identified where the organization's "main establishment" (the organization's main facility in the EU where most of personal data is processed and stored) is likely to be considered as relevant for all GDPR requirements?	100
Does the organization assess the likelihood of being at risk with regard to the processing of personal data and associated liability issues with respect to the "main establishment" (the organization's main facility in the EU where most of personal data is processed and stored)?	0
Did the organization formally appoint an EU representative to operate as the local liaison with data subjects and supervisory authorities as required by GDPR?	0
When the organization stores, processes or transmits EU residents' data, does the organization ensure that data is protected as defined in the GDPR?	0
Does the organization utilize any internal or external services to track and monitor any EU Residents' data?	100
Article 4: Definitions	50
Has the organization identified where the organization's "main establishment" (the organization's main facility in the EU where most of personal data is processed and stored) is likely to be considered as relevant for all GDPR requirements?	100
Does the organization assess the likelihood of being at risk with regard to the processing of personal data and associated liability issues with respect to the "main establishment" (the organization's main facility in the EU where most of personal data is processed and stored)?	0
Chapter 2: Principles	**10**
Chapter 2: Principles	10
Article 5: Principles relating to personal data processing	50
Has the organization established guidelines, baselines or any other directive measure to embed a Privacy by Design principle when	100



STEP 4:
TAKE ACTION

Once provided with your organizations analysis regarding GDPR, you will be provided with recommendation and remediation steps that should be performed to increase the compliance level with the GDPR requirements.

Automated Cyber Risk Officer (ACRO) by Ctegic

Security is not a technology issue – it's a financial issue! In an asymmetric world where an attack may cost a fraction of defenses, putting your funds and people where it really matters is an imperative. Cytegic's ACRO enables business executives to make the financial decision between risk reduction by investments in defenses and/or risk hedging by cyber insurance. With ACRO cyber risk is just another business decision. ACRO enables organizations to gain efficiency, reduce costs and hedge risk.

CONTACT CYTEGIC

For more information about Cytegic
please visit our website at **www.cytegic.com**

To schedule a meeting with a Cytegic representative contact:
Phone: +972-52-5221170, eMail: elon.kaplan@cytegic.com