

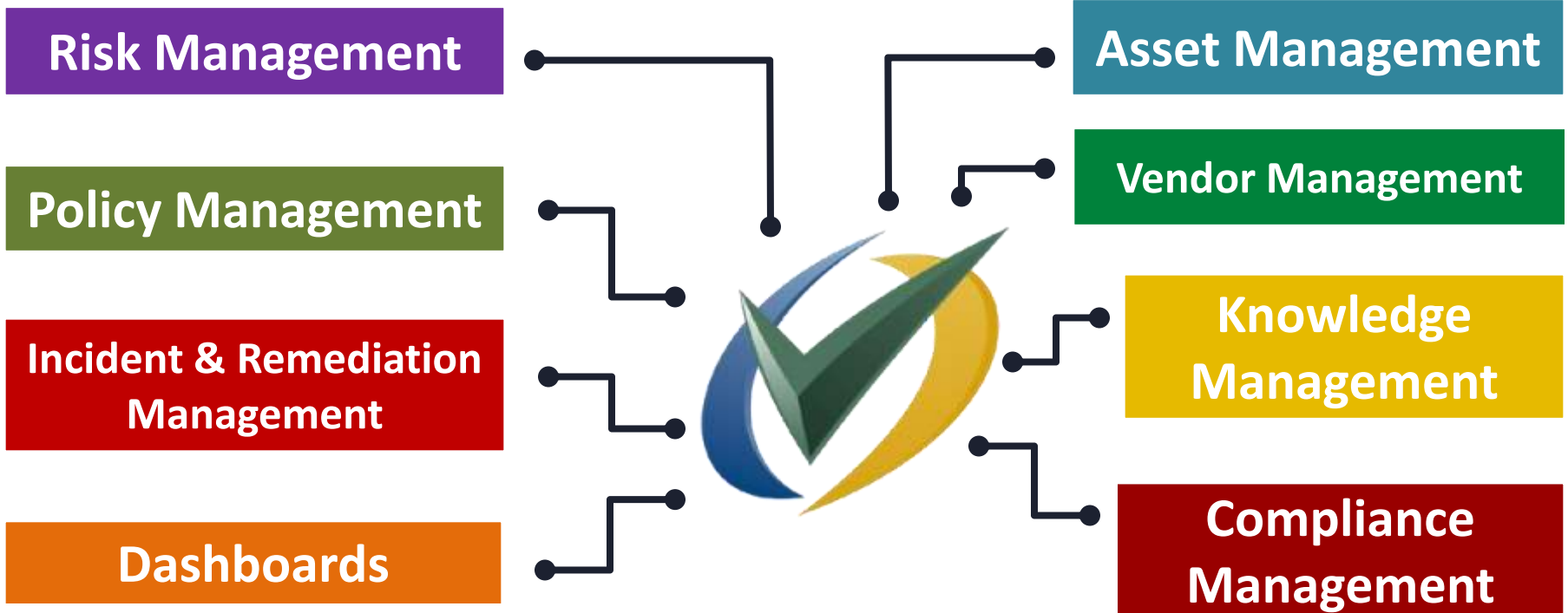
Using OVAL for Information Security Application Integration

Marlon Gaspar
Senior Software Architect
mgaspar@modulo.com

About Modulo

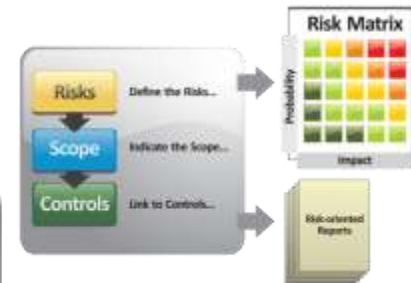
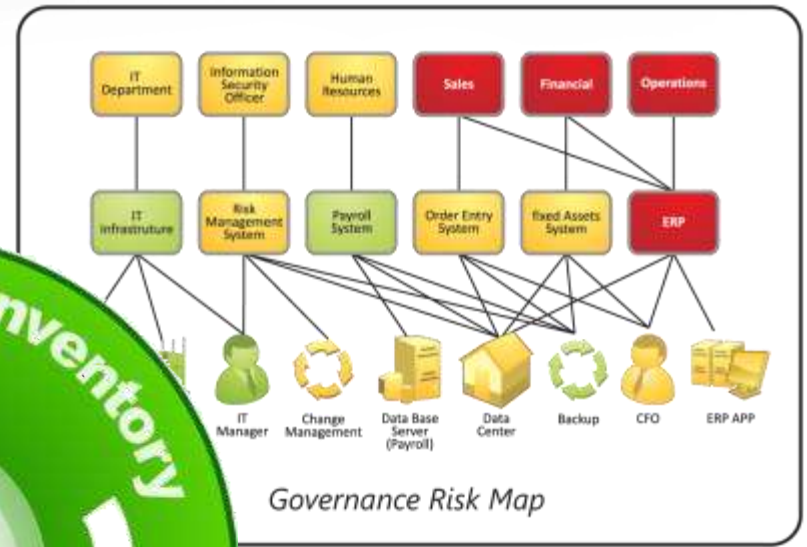
Modulo is the leading global IT GRC software provider based in Brazil with North American operations in Atlanta. We provide a SaaS or on-premise solution for IT Risk and Compliance needs in every major vertical market, serving Fortune 1000 clients. Modulo was recently awarded the top ranking in IT GRC solutions by SC Magazine. The June issue of CSO magazine features a cover article of our client, Synovus Financial, and their risk management automation program using Modulo Risk Manager.

Modulo Comprehensive GRC Solution



Modulo – Copyright © All rights reserved

Modulo GRC Metaframework



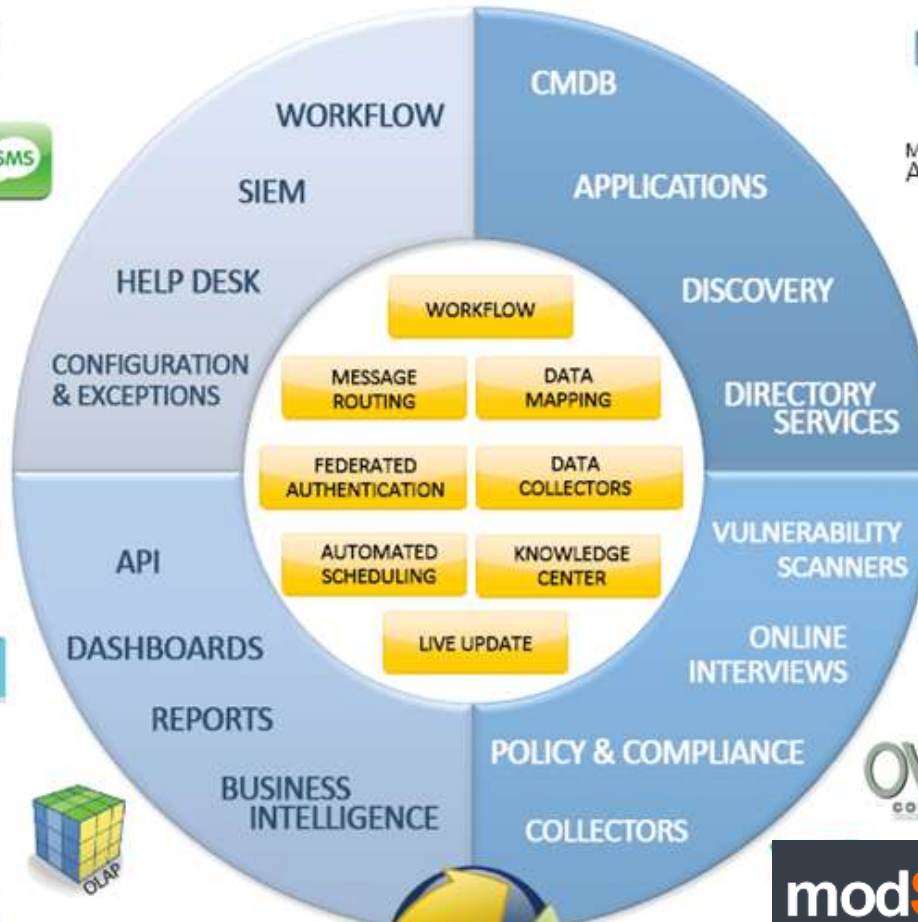
Modulo Risk Manager Integrations

TREATMENT

INVENTORY



EVALUATION



Microsoft Active Directory

Microsoft System Center



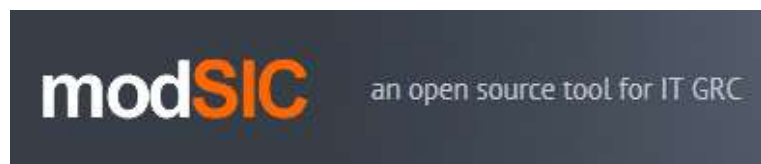
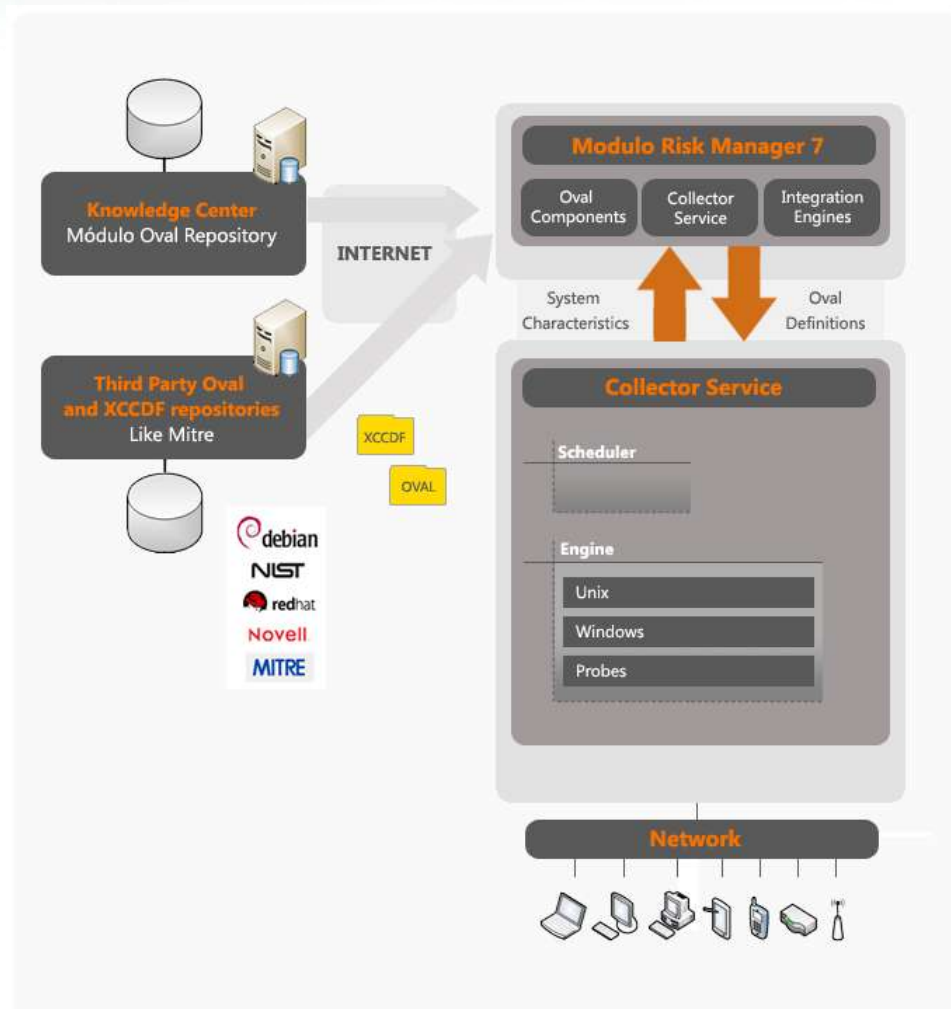
ANALYSIS



MODSIC OVAL Collectors

<http://www.modsic.org>

- ✓ **Modulo Open Distributed SCAP Infrastructure Collector (modSIC):** Open Source collection and assessment service for technology assets based on the open SCAP (Security Content Automation Protocol) standard.



Integrating Information Security Applications

In order to **Continuous Monitor**
a complex environment risk
posture, you need to **integrate**
multiple assessment solutions.

Security in a constantly changing environment

What you need

- 1. Choose the right integration layer**
- 2. Model your data**
- 3. Build the connector**
- 4. Harmonize your risk indicators**

SAP ABAP Integration

What you need

- 1. Choose the right integration layer**
2. Model your data
3. Build the connector
4. Harmonize your risk indicators

Know your objectives

Find the frictionless path

SAP Integration

Integration in the analysis layer, feeding Risk Manager with the current control state of the systems.

What you need

1. Choose the right integration layer
2. **Model your data**
3. Build the connector
4. Harmonize your risk indicators

Leverage OVAL existing constructs

SAP Integration Schema

The screenshot displays the SAP Integration Schema tool interface. At the top, a tab is labeled 'sapcode_object' with an extension icon and the text 'extension + oval-def:ObjectType'. Below this, a list of attributes is shown. The 'system_name' attribute is highlighted with an orange border. The interface includes a left sidebar with icons for 'extension', 'sequence', 'choice', and 'S...', and a main table of attributes.

Attribute	Value
@ id	oval:ObjectIDPattern
@ version	xsd:nonNegativeInteger
@ comment	oval:NonEmptyStringType
@ deprecated	xsd:boolean
ds:Signature [0..1]	ds:SignatureType
notes [0..1]	oval-def:NotesType
oval-def:set	
system_name	oval-def:EntityStateStringType
issue	oval-def:EntityObjectIntType

SAP Integration Schema

The screenshot displays the SAP Integration Schema for the `sapcode_item` extension of `oval-sc:ItemType`. The schema is shown in a tree view with a list of elements on the right. The elements are:

- `@ id` (required) with type `oval:ItemIDPattern`
- `@ status` (required) with type `oval-sc:StatusEnumeration`
- `<> message [0..50]` (optional) with type `oval:MessageType`
- `<> system_name` (optional) with type `oval-sc:EntityItemIntType`
- `<> issue` (optional) with type `oval-sc:EntityItemIntType`
- `<> total_issues_found` (optional) with type `oval-sc:EntityItemIntType`
- `<> total_programs_scanned [0..1]` (optional) with type `oval-sc:EntityItemIntType`
- `<> evidence [0..*]` (optional) with type `oval-sc:EntityItemStringType`

The `system_name`, `issue`, `total_issues_found`, `total_programs_scanned`, and `evidence` elements are highlighted with an orange border. The left sidebar shows the schema structure with `extension oval-sc:ItemType` and two `sequence` containers.

What you need

1. Choose the right integration layer
2. Model your data
3. **Build the connector**
4. Harmonize your risk indicators

OVAL modular design allows easy extensibility

SAP Integration

modSIC plugin extends OVAL
schema and collection
capabilities to support the
ABAP code scanning

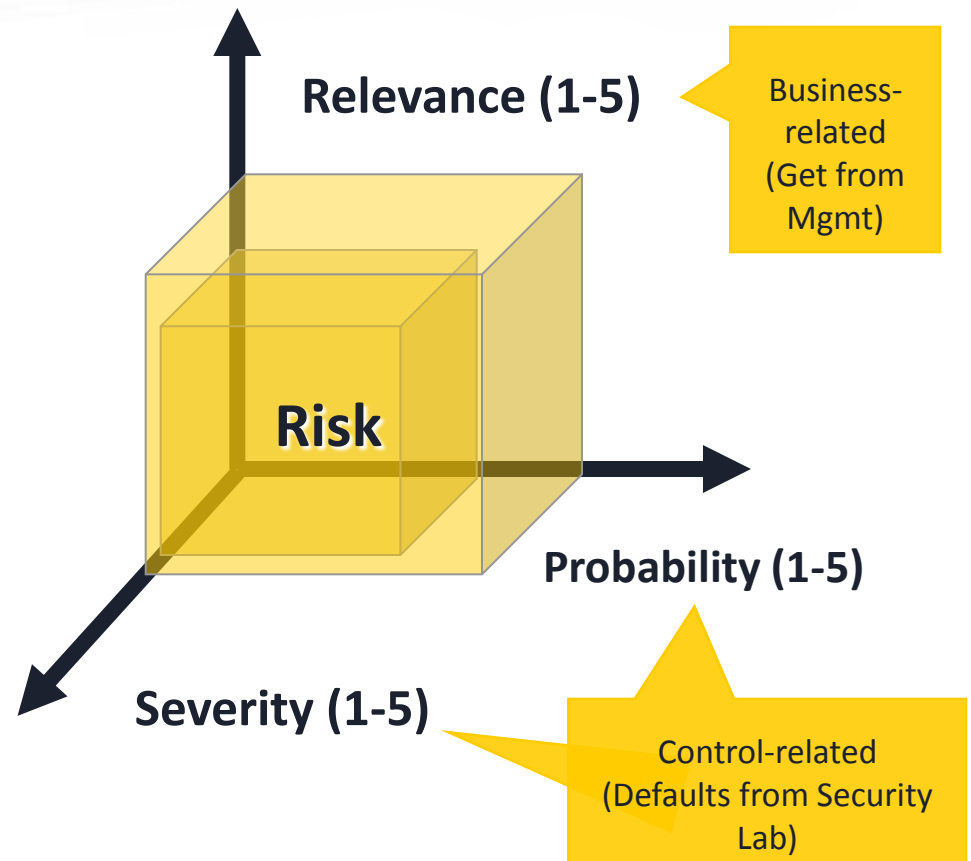
What you need

1. Choose the right integration layer
2. Model your data
3. Build the connector
4. **Harmonize your risk indicators**

Risk Calculation (PSR[®] – Risk Index)

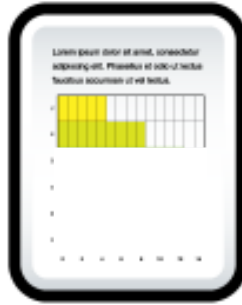
ISO IEC	
RISK LEVEL	PSR [®] VALUES
Very Low	1, 2, 3, 4, 5, 6
Low	8, 9, 10, 12, 15, 16
Medium	18, 20, 24, 25, 27, 30
High	32, 36, 40, 45, 48, 50
Very High	60, 64, 75, 80, 100, 125

Vocabulary — Guidelines for use in standards
 Management du risque —
 Vocabulaire — Principes directeurs pour l'utilisation dans les normes



$$\text{RISK} = \text{P} \cdot \text{S} \cdot \text{R}$$

Harmonize the data into a single Risk Score



PSR
PSR
PSR
PSR
PSR

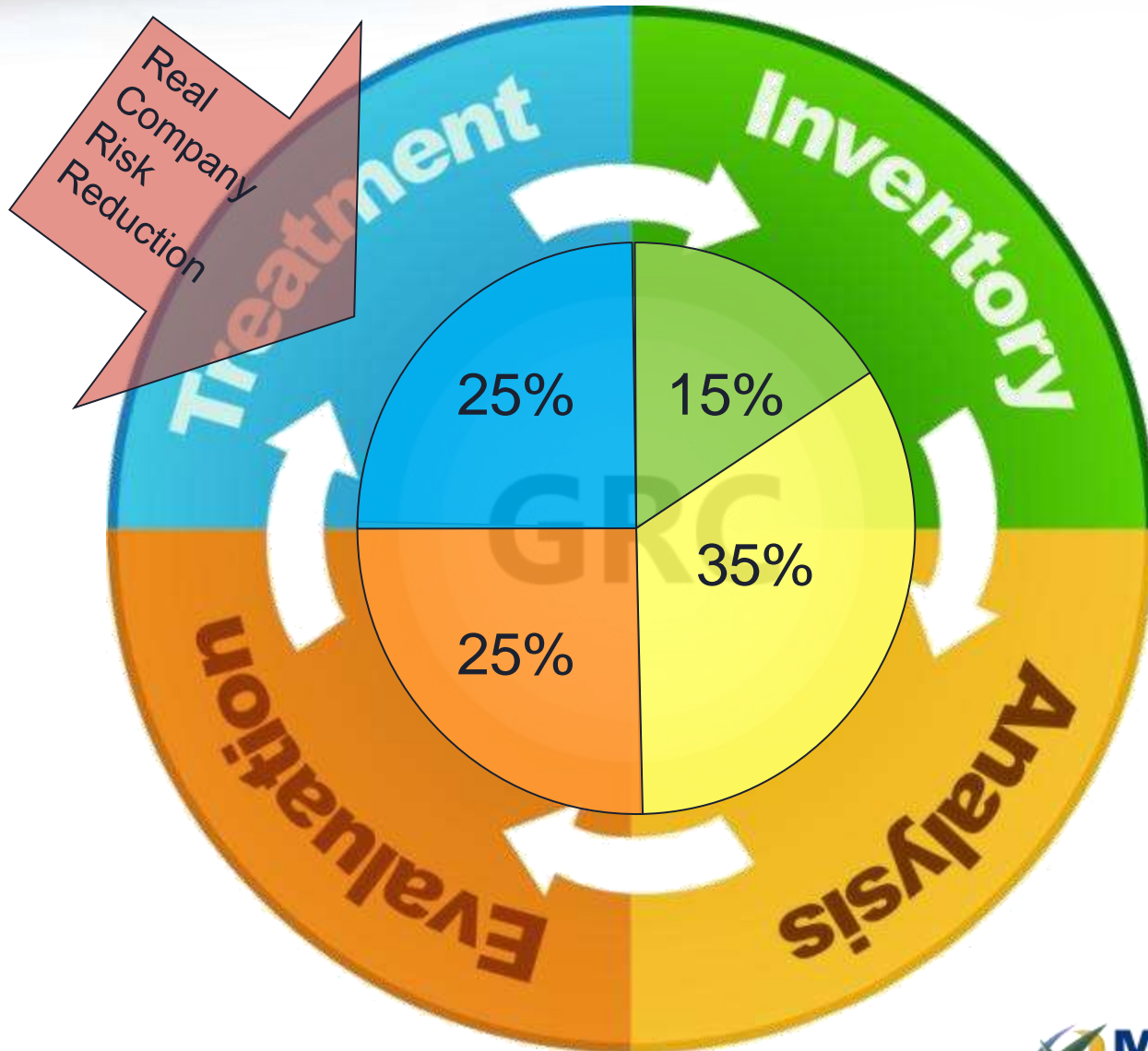


RM Project Manager

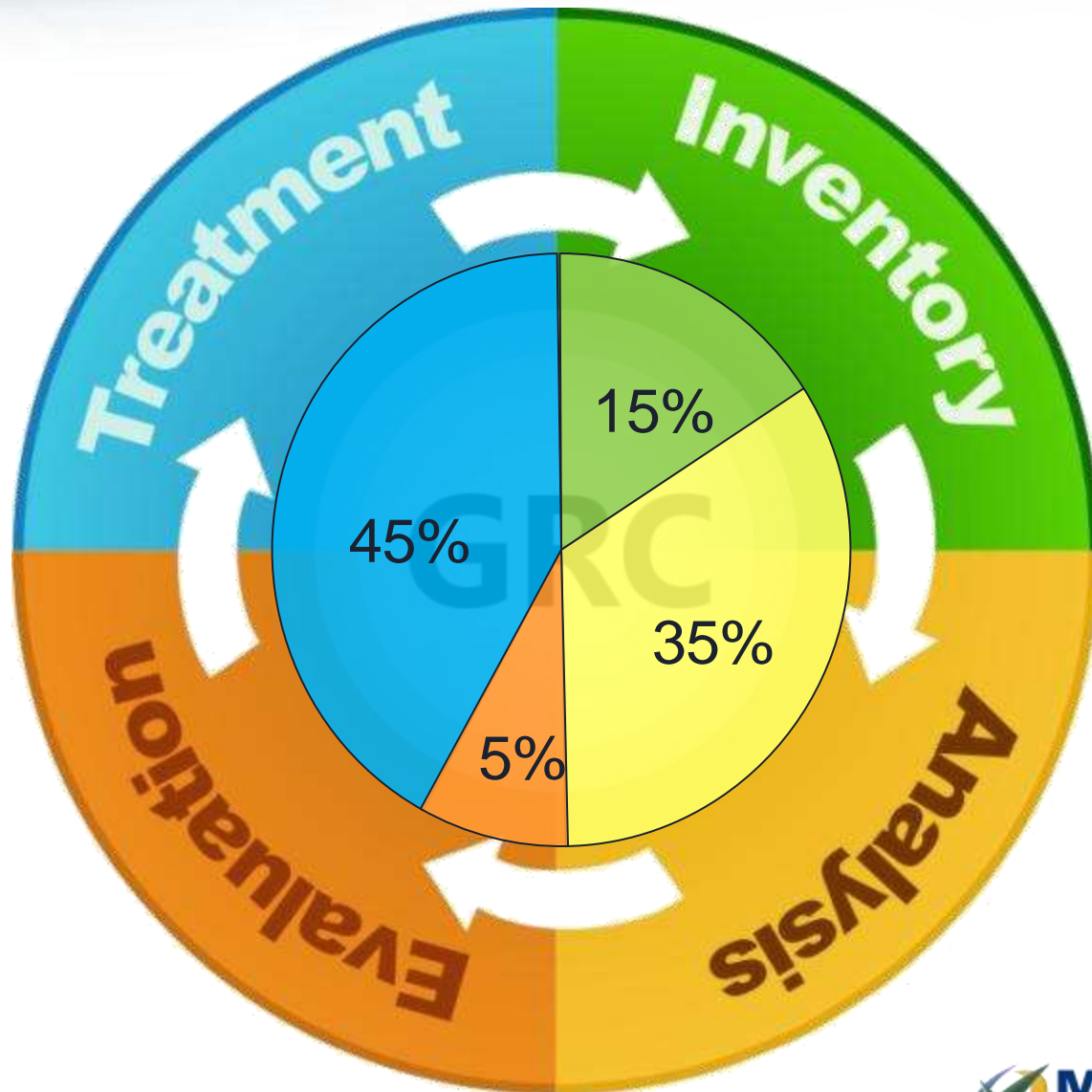


DEMO

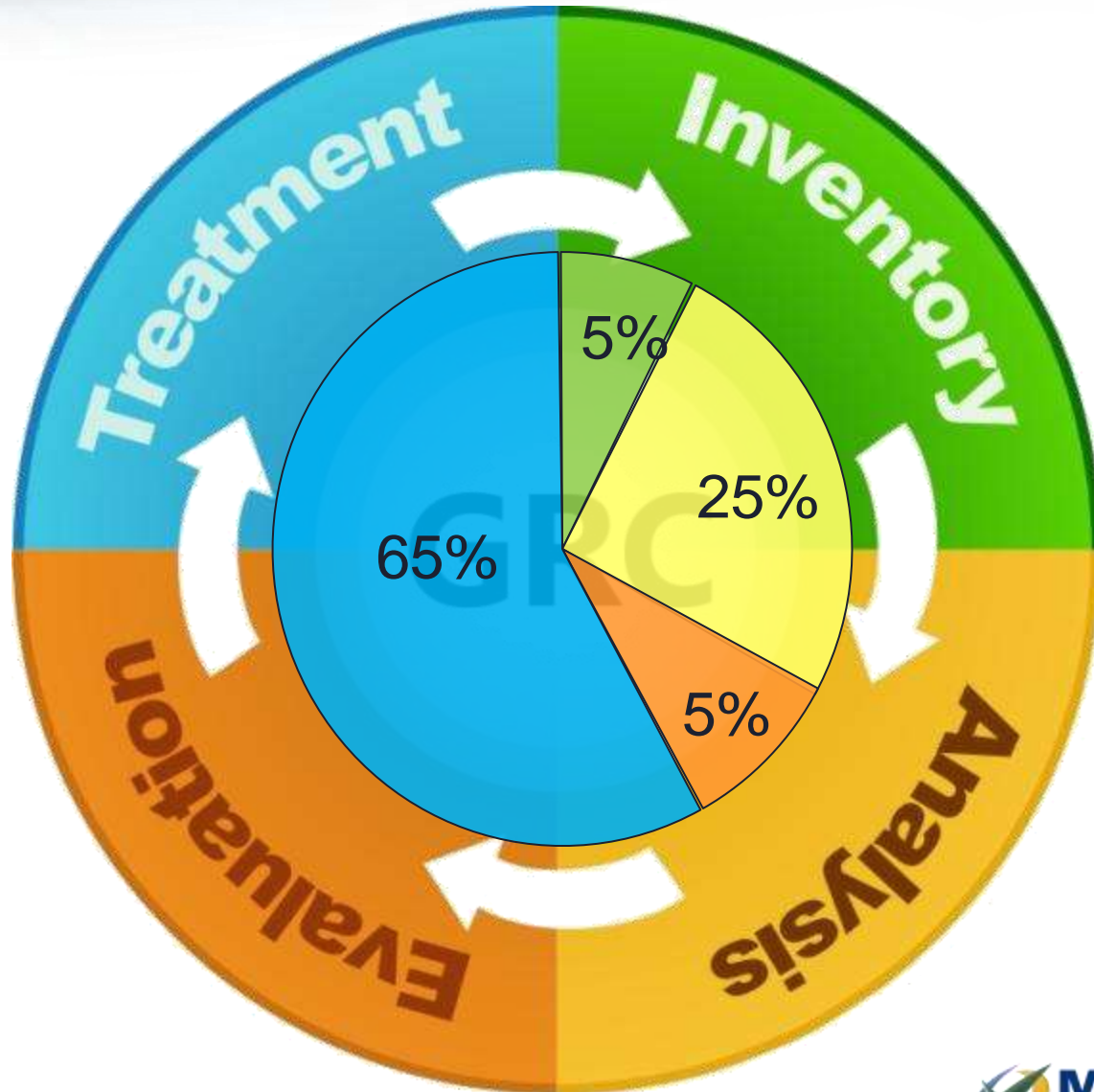
Manual Risk Management Process



Automated Process First Year with Modulo



Automated Process Second Year with Modulo



Questions?

THANK YOU

Marlon Gaspar
mgaspar@modulo.com