GRMA

GOVERNANCE & RISK MANAGEMENT APPLICATION

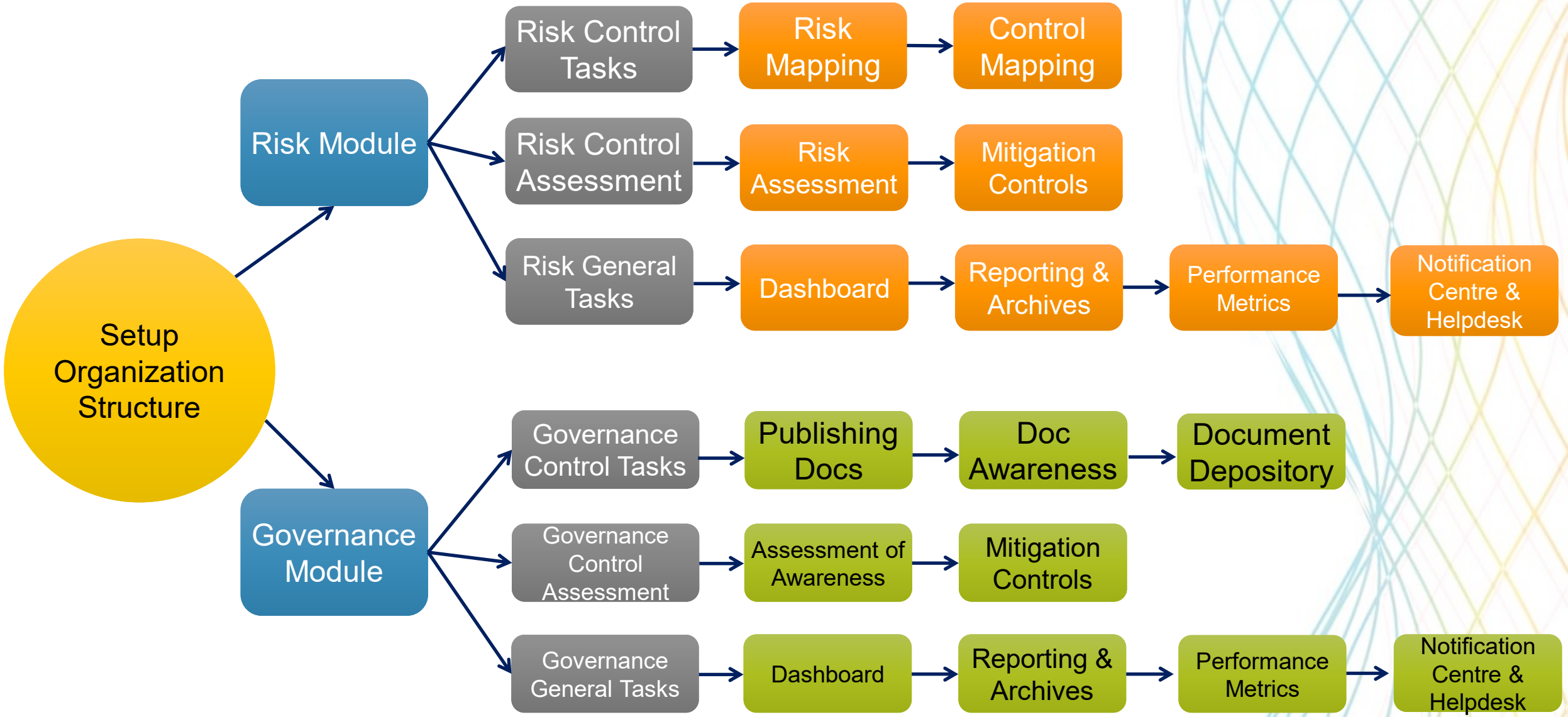
DEVELOPMENT STAGE

ProBuds
Strategy Consulting
Consulting | Compliance | Risk | Management

ISO 27001:2013 CERTIFIED

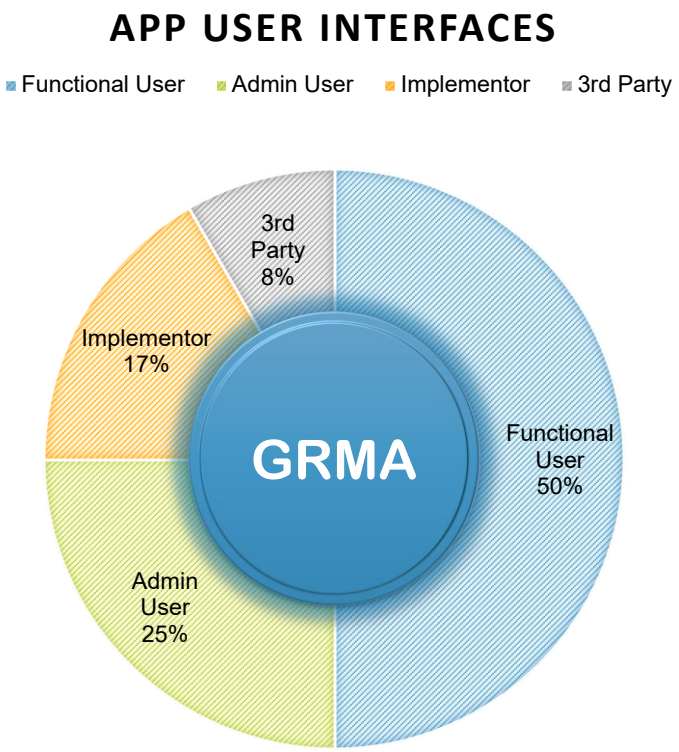
ISO 9001 CERTIFIED

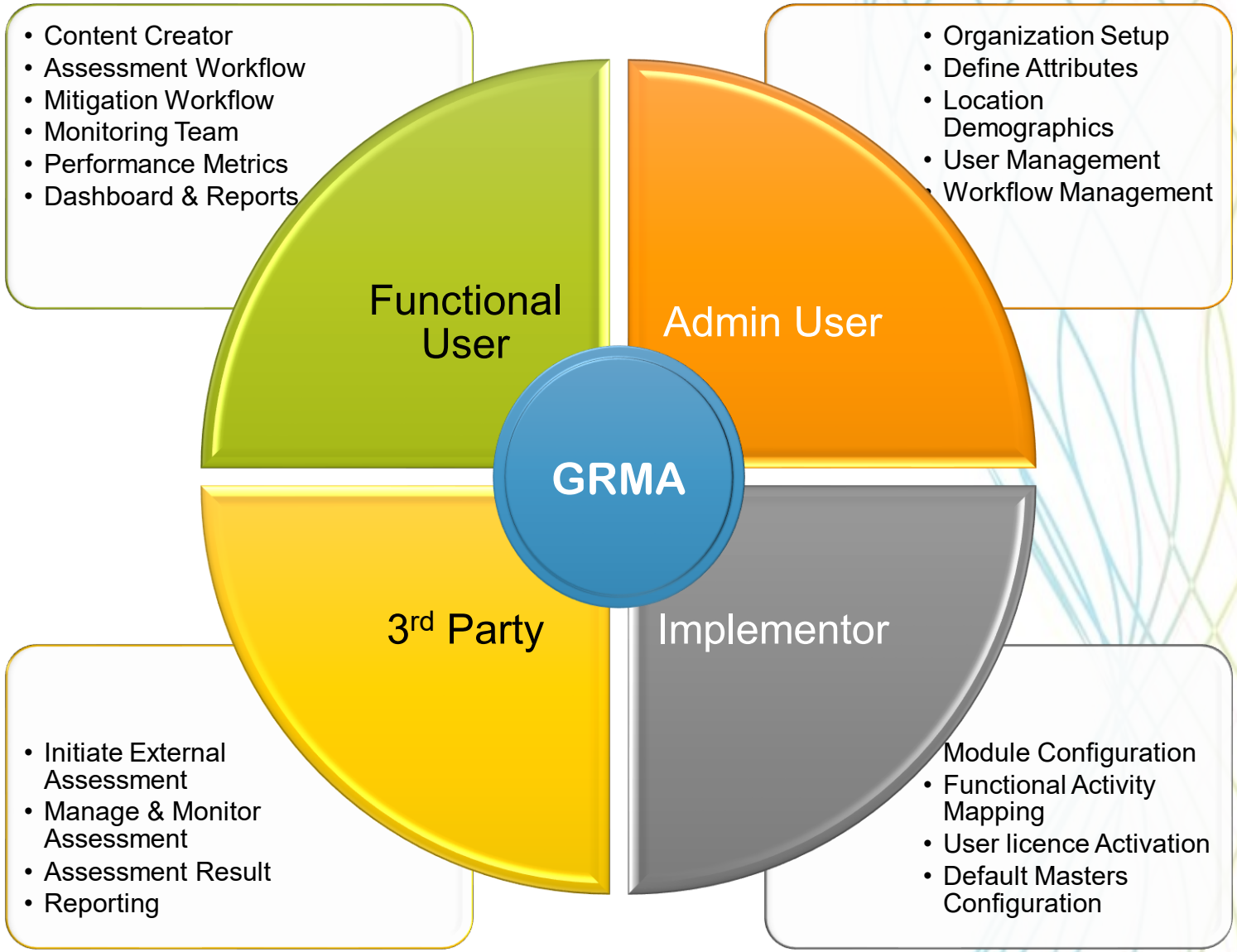
Overview of Concept Flow* of GRMA



* This process flow is indicative only. Please expect changes after project study is complete

Overview of User Interfaces* in GRMA





* This process flow is indicative only. Please expect changes after project study is complete

Requirement Brief for App Development -1

- 2 factor user authentication security login
- Account Management
- User Management
- Role-based access to all users across locations/ zones
- Creation and Administration of Content/ Data Library as per Data Types defined
- Content examples, policies, risk controls, report templates, reference documentation, etc
- Pre-defined risk libraries for control assessment
- Define Risk Assessment Procedures
- Create Risk Scenarios/ Policy Statements
- Risk control self-assessment checkflows
- Controls can be documented, assigned to responsible users and departments, and associated with the risks they mitigate
- Risk based on segments/ transaction types
- User Workflow Management for various functional activities
- Workflow for Heat Map and Risk Register Approval
- Action/ Mitigation Plans and Specific Controls Mechanism
- Defining Risk Management Policies
- Creating Risk Control Matrices (RCM) and its mapping to all department users
- The solution provides the built-in ability to document control activities currently in scope and perform validation testing such as Control Self Assessments, Design Efficiency and Operating Efficiency testing, etc
- Integration of Risk Register with 3rd party applications through API's
- Create user defined questionnaires from a provided library of questions to build up as Risk based Question Bank.
- Map risk assessment questionnaires to business hierarchy and/or business assets
- Build and execute risk assessments in the form of questionnaires
- The solution supports a master library of questions that can be used in multiple questionnaires and are mapped to standards/frameworks
- Alert / Notification Control Centre
- Manage and Report Audit Log/ Trail

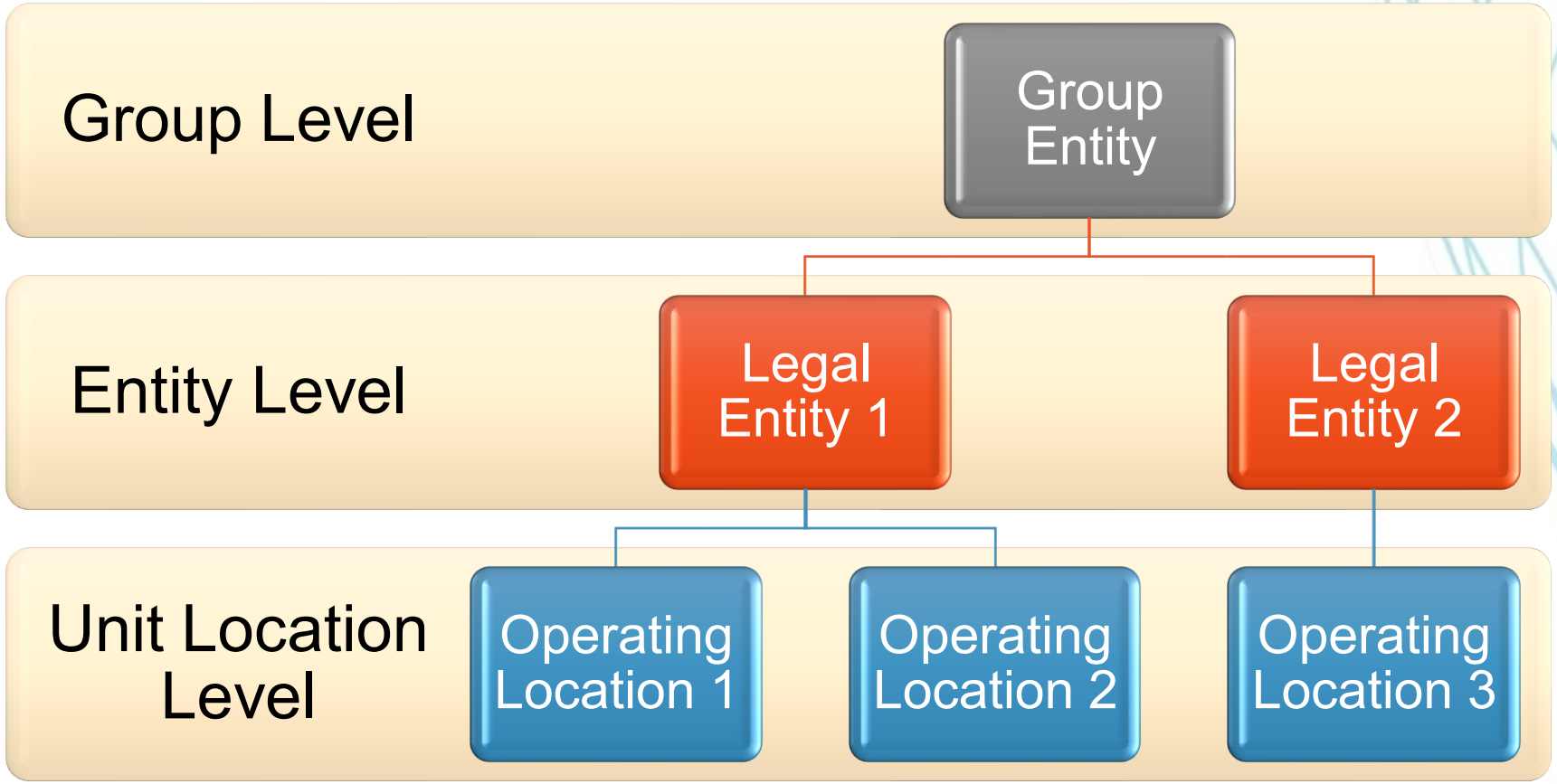
Requirement Brief for App Development -2

- **Function based User Controls:**
- Ability to have Dashboards, such as, 5x5 Risk Heat Map, Key Risk Indicator (KRI)Analysis, Business Impact Analysis, Risk vulnerabilities by Priorities, etc
- Customized Dashboards, like, Risk Analysis Output for Inherent, Residual or anyuser defined risk types (use of histogram/ pareto/ spider/ scatter/ trend plots, wherever possible)
- Comprehensive Report Management
- Qualitative risk rating (eg, by inherent/ residual/ defined types)
- Development of Risk Register
- Ability to create online Risk Register
- Ability to Update Risk Register
- Risk Assessment Study of all Departments
- Assessment through Risk Control Templates
- Ability to conduct Risk & Controls Self-Assessment online by departments/ projectrepresentatives
- Risk likelihood and impact can be assessed for both inherent and residual risk acrossmultiple risk categories using monetary values
- Escalation Matrix to escalate issues to ensure proper sign-off/ approval of issues forOrganized or managed processes
- The solution provides the ability to raise change requests related to risk statements/policy statements
- The solution provides the ability to create campaigns to drive policy awareness &education efforts and capture policy acknowledgements
- The survey functionality includes the ability to assign multiple recipients from a singletemplate and reporting across different departmental entities
- The solution includes built-in weighting/ scoring capabilities to allow for easyprioritization of business-critical compliance requirements
- Ability to provide built-in assessments and questionnaires as well as manually createassessments and questionnaires per defined guidelines for conducting compliance testing
- Provide a mechanism to track and remediate control deficiencies identified duringtesting
- Schedule Management - The solution provides annual compliance confirmations/ trainings which can be rolled out to employees with respect to Policy awareness orrisk assessment

Important Points for App Development

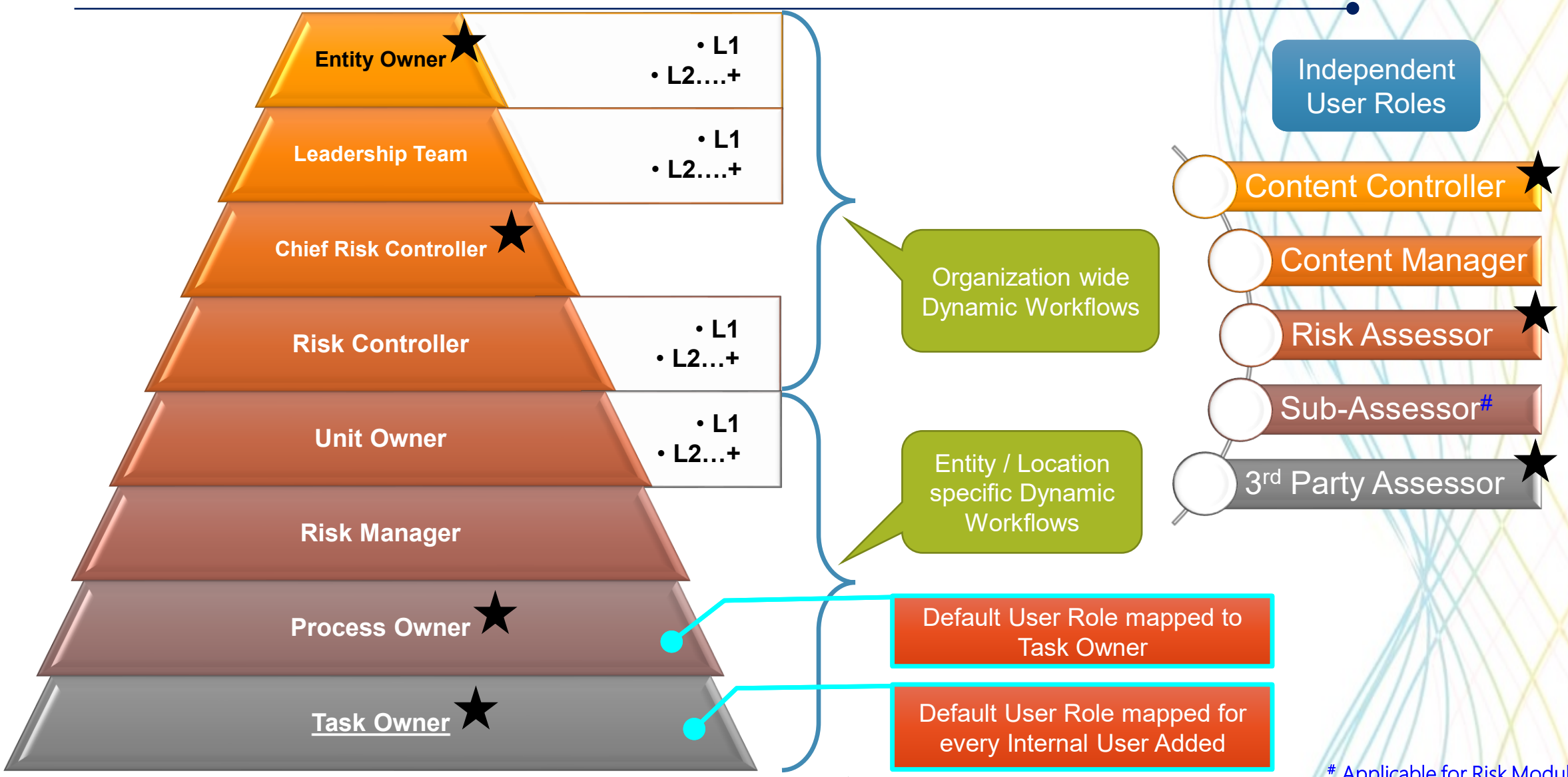
- Major Browser's compatibility to be there, like, Chrome, Edge, Safari, Firefox, etc. with 'Mobile Site View' browser settings.
- Primary Application Server to be reliable Open Source , but open to integration with other licensed versions of Application Servers, as per the customized requirement of clients. Like Apache Tomcat.
- Primary Database to be MySQL, but compatibility with major Databases, like latest versions of Oracle, SQL, SAP HANA, IBM DB2 (Database to be selected as per the requirement of clients)
- Data Structure to be designed for swiftness, efficiency, accuracy, flexibility, responsiveness
- User interfaces to be simple but effective in features and versatile in its use.
- Network Security is of utmost importance. Web address to be https, and data / credentials to be transmitted through highly encrypted channel (like, AES 128-bit encryption, etc), and adequate Firewalls (each on Application Server and Database) to protect the Servers from being compromised. **Detailed Security Architecture document to be made available by Developer**.
- Port visibility for internal server implemented
- Configuring HTTP Strict Transport Security (HSTS) on web server to be implemented to avoid cookie hijacking
- Configuring Ciphers with strong authentication
- VPN Connection compatibility to be available. To be implemented / configured as per clients requirements only.
- Two step verification option should be configured with Yes and No options and settings
- Content Type Verification is required by running anti-virus scan at Server side, before data is archived. Only selected MIME Types to be allowed with help of white listing. Files uploaded should not be uploaded inside the server root.
- Application should be easily configurable for SSO (Single Sign on) integrations, like OKTA, AD, etc (to be selected as per the requirement of clients)
- Protection against vulnerable click jacking attacks, hacking threats, SQL script injections, Java scripts, or any sort of Cross site scripting attacks, to be essentially available
- Flexibility towards implementing Password Policy Management, like combination passwords to be allowed, before changing to new password, old password required, etc
- List of API integrations to be available
- Offline Network Compatibility to be explored. Application should display whether its working on Offline mode or Online mode.
- Application Architecture should pass through all parameters of VAPT

Overview of Organization Setup* in GRMA



* This process flow is indicative only. Please expect changes after project study is complete

Overview of 13 User Roles* in GRMA



Applicable for Risk Module

★ ***Default User Role at the time of Setup***

** This process flow is indicative only. Please expect changes after project study is complete*

Functional Mapping* (scenario example)

Registered Licence User	Dept	User*	Entities** mapped	Unit locations*** mapped
GROUP Global/ Logical/ Group Entity (Registered Licensee) Unique Code allotted/ created at the time of registration/ implementation	HR FIN Department(s) IT RISK	U1 U2 User(s) U3 U4	Leg Ent 1	Loc 1 Loc 2 Loc 3
			Leg Ent 2	Loc 1 Loc 2
			Leg Ent 3	Loc 1 Loc 2

* Number of Users added will depend upon the inputs by Implementor on User Licence Registration Page

** Number of Entities added will depend upon the inputs by Implementor on User Licence Registration Page

*** Number of Unit Locations added will depend upon the inputs by Implementor on User Licence Registration Page

* This process flow is indicative only. Please expect changes after project study is complete

Steps involved for implementing GRMA* (illustrative list)

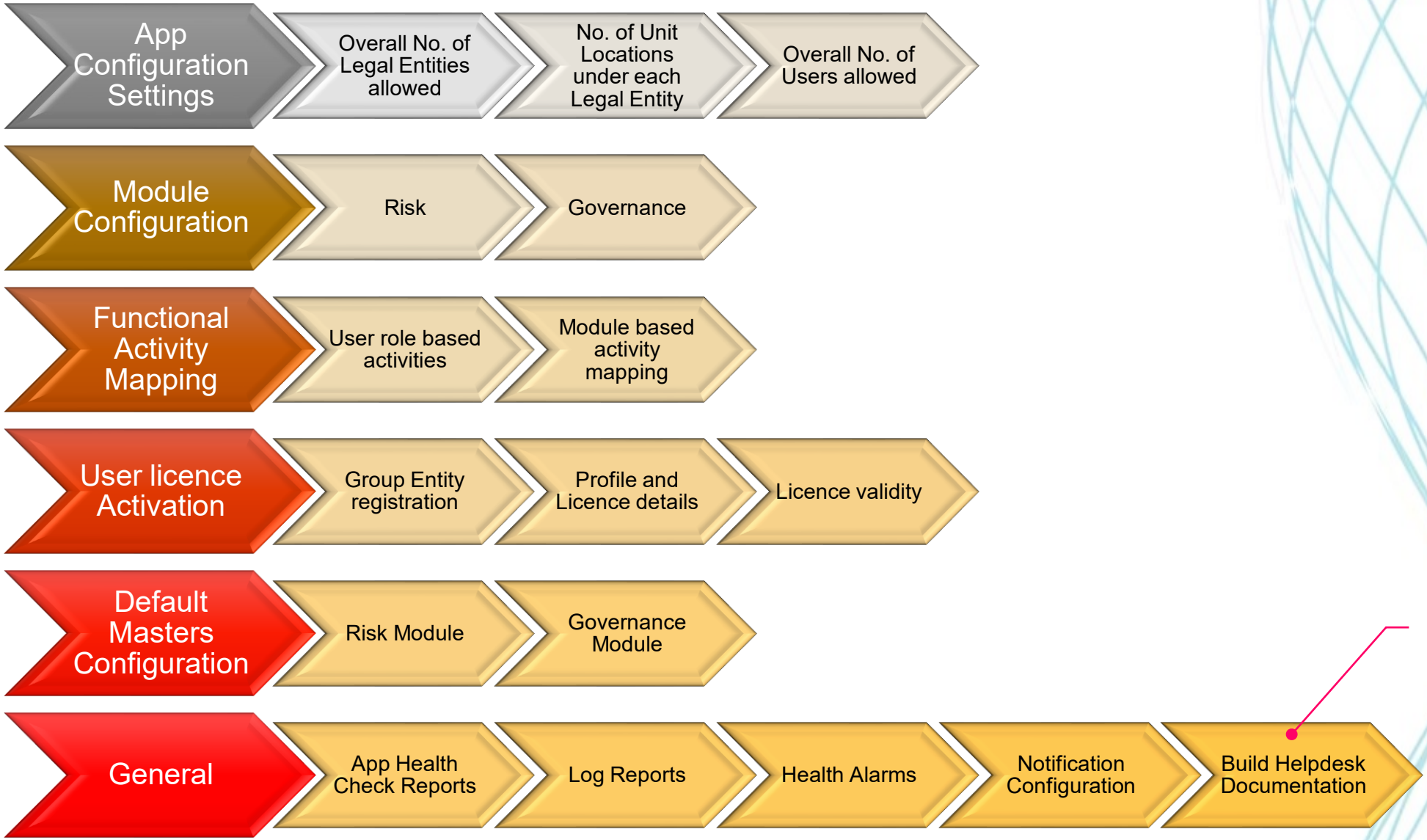
- Get Customer details for registration in Developer Console/ Webpage
- Generate an unique “License Key” for completing online registration and payment details through Developer Console. Registrant will receive an email regarding activating the License Ley.
- License Key remains validated for 7 days. If License Key is “Activated” within 7 days, the status changes to “Active”, else the status remains “Inactivated”. The License Key will need to be “Revalidated” after 7 days, to be again activated within next 7 days. There will be 5 Status of License Key, namely, Inactivated, Activated, Revalidation Required, Suspended, Terminated.
- Server Set up process to begin, with Network configuration, security framework, aligning with application architecture
- Once setup is complete, Application installation takes place
- EULA needs to be consented at this stage. EULA will be integrated to application.

EULA - (End User License Agreement)

  1. Details from Registration form are used,
  2. Enter “License Key” for matching with registered records (only “Activated” status applicable),
  3. The registrant will receive an “OTP” to confirm the activation and acceptance of EULA. EULA will capture the IP Address of the Server, Message ID through which OTP was communicated (to retain the authenticity)
  4. Only the active licence to be used for further configuration.
  5. Copy of EULA to be sent to registered user mail id and one copy to be archived with ProBuds for future records.
  6. Application will run seamlessly if EULA with License Key Status is “Activated” all the time.
- Implementor to Begin functional configuration setup

Overview of Process Flow* of User Interface in GRMA

IMPLEMENTOR



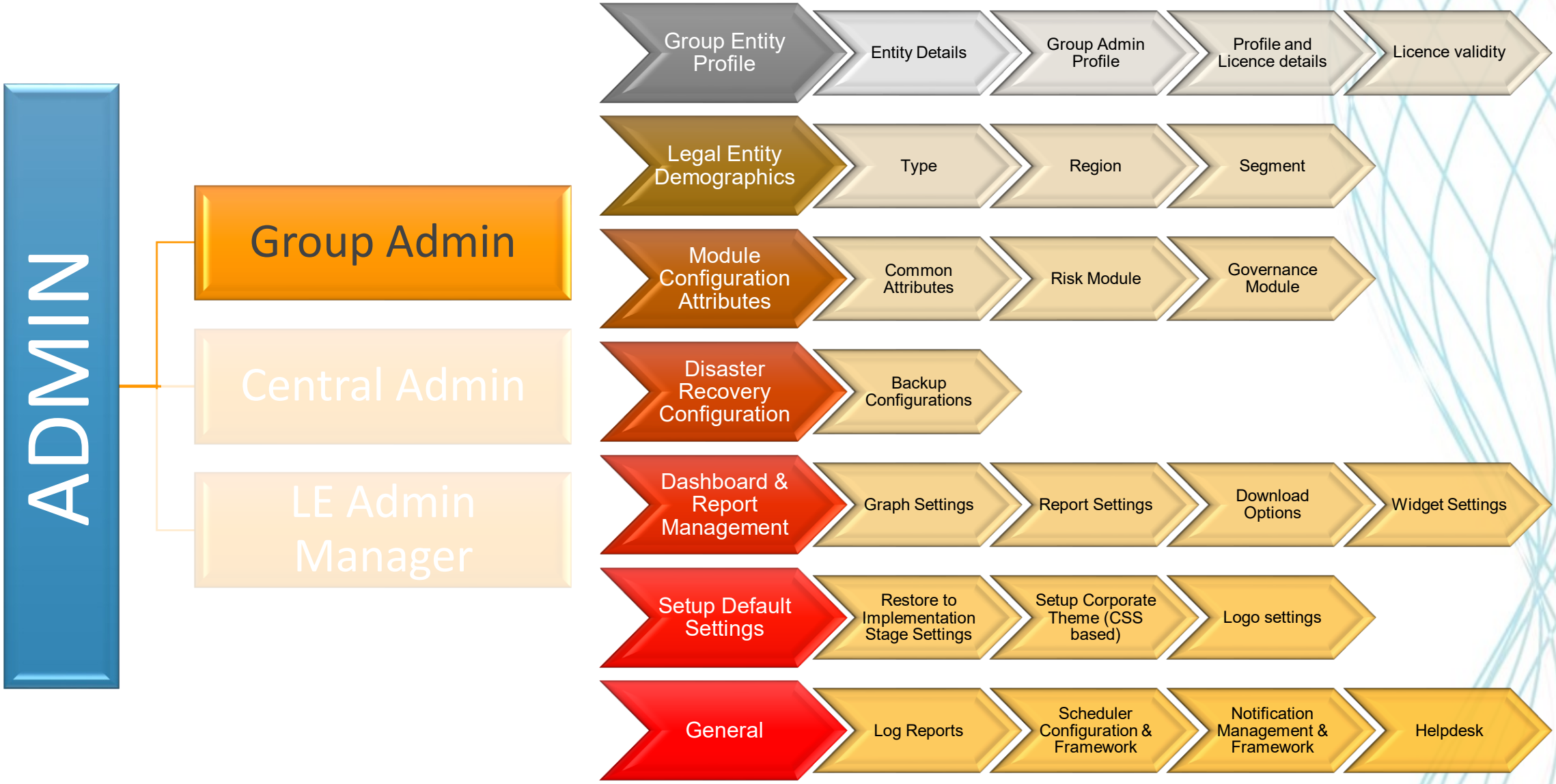
* This process flow is indicative only. Please expect changes after project study is complete

Steps involved for function setup of GRMA* (illustrative list)

- Implementor to Begin functional configuration setup
- Masters to be built
- Content to be uploaded
- Mapping to be done
- Test the data with client UAT Acceptance Criteria
- Training of modules and workflows to be given and client sign off to be taken
- Implementation complete
- Fill in the Support Service webpage with implementation details, like, GoLive Date, Free Period, Start of Paid Support, Validity of Support, obligations, etc.
- The Support Service for registrant needs to be updated at Application level as well. There will be 4 Status of Support Service, namely, Free Period, Active, Suspended, Terminated.
- In the event of Account being Suspended or Terminated, the resumption of support service can happen upon confirmation through OTP.

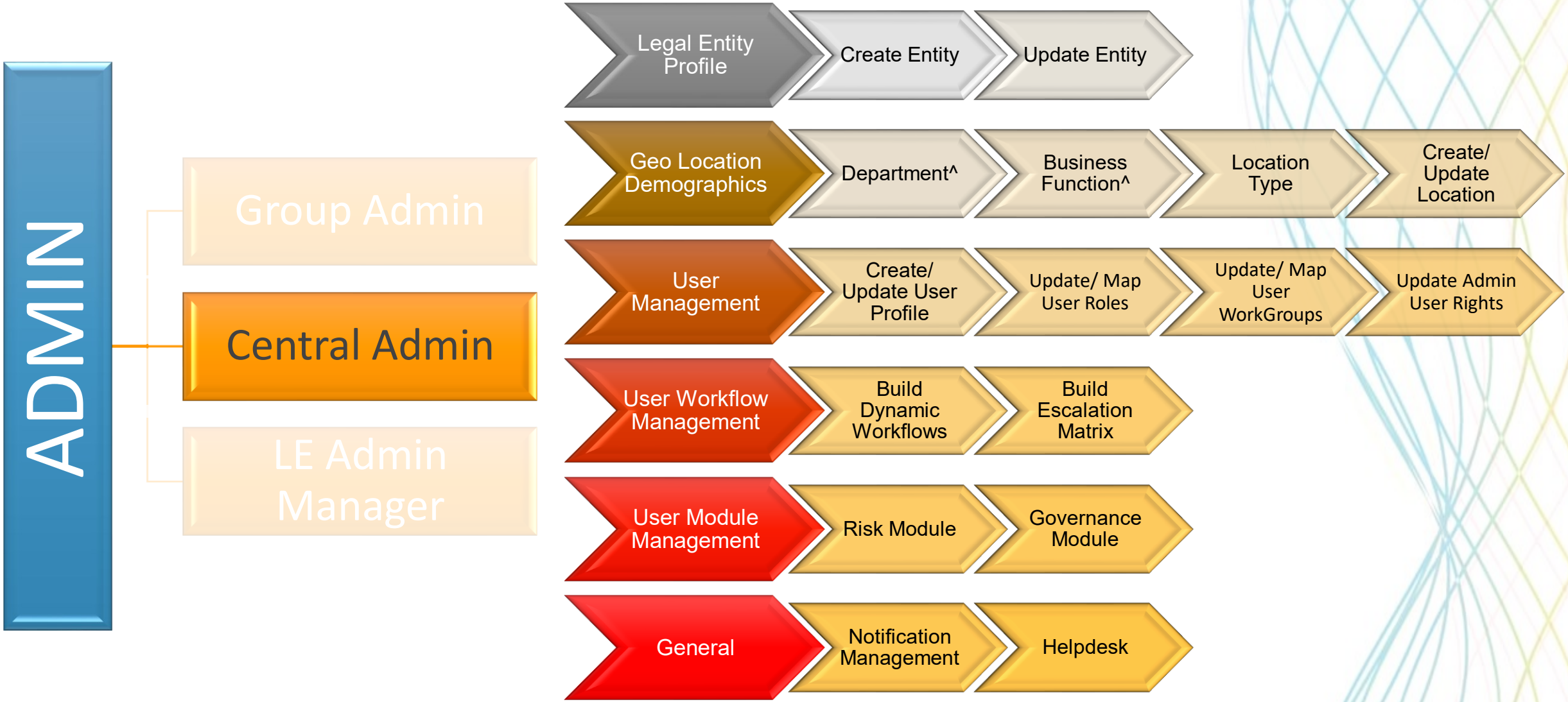
** This process flow is indicative only. Please expect changes after project study is complete*

Overview of Process Flow* of User Interface in GRMA



** This process flow is indicative only. Please expect changes after project study is complete*

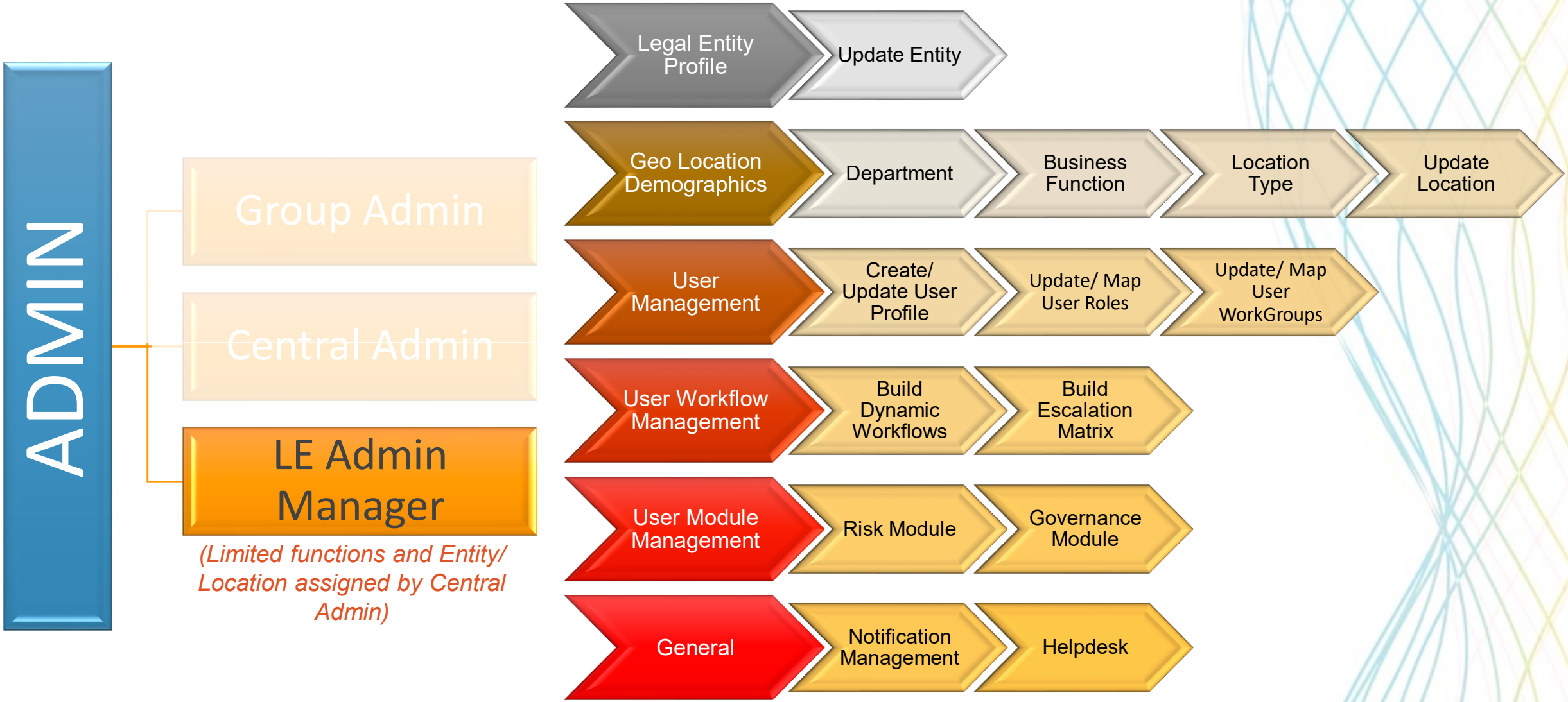
Overview of Process Flow* of User Interface in GRMA



^ *Department Name can be used as Business Function as well (doesn't need to be added again*

* *This process flow is indicative only. Please expect changes after project study is complete*

Overview of Process Flow* of User Interface in GRMA



* This process flow is indicative only. Please expect changes after project study is complete

Overview of Process Flow* of User Interface in GRMA

FUNCTIONAL USER

- Entity Owner
- Risk Controller
- Unit Owner ★
- Risk Manager ★
- Process Owner
- Task Owner
- Content Controller
- Content Manager
- Risk Assessor

RISK MODULE

Task Dashboard	
Action Board	•Assessment Result & Mitigation •Assessment Monitoring/ Reporting
Risk Performance Metric	•Overall Performance •Impact of KRI's
Risk Register	•View Risk Register •Request Changes
Risk Control Matrix	•View Risk Register •Request Changes
Question Bank	•Add/ Edit/ View Questions
Assessment Archives	
Notification & Alerts	
Helpdesk	

GOVERNANCE MODULE

Task Dashboard	
Action Board	•Assessment Result & Mitigation •Assessment Monitoring/ Reporting
Governance Performance Metric	
Question Bank	•Add/ Edit/ View Questions
Assessment Archives	
Notification & Alerts	
Helpdesk	

★ Example of additional User roles

* This process flow is indicative only. Please expect changes after project study is complete

Overview of Process Flow* of User Interface in GRMA

FUNCTIONAL USER

- Entity Owner
- Risk Controller
- Unit Owner
- Risk Manager
- Process Owner
- Task Owner
- Content Controller
- Content Manager
- Risk Assessor

RISK MODULE

Task Dashboard	
Action Board	•Initiate/ Manage Assessment •Assessment Result & Monitoring •Assessment Reporting
Risk Performance Metric	•Overall Performance •Impact of KRI's
Risk Register	•View Risk Register •Request Changes
Risk Control Matrix	•View Risk Register •Request Changes
Question Bank	•Add/ Edit/ View Questions
Assessment Archives	
Notification & Alerts	
Helpdesk	

GOVERNANCE MODULE

Task Dashboard	
Action Board	•Initiate/ Manage Assessment •Assessment Result & Monitoring •Assessment Reporting
Governance Performance Metric	
Question Bank	•Add/ Edit/ View Questions
Assessment Archives	
Notification & Alerts	
Helpdesk	

** This process flow is indicative only. Please expect changes after project study is complete*

Overview of Process Flow* of User Interface in GRMA

FUNCTIONAL USER

- Entity Owner
- Risk Controller
- Unit Owner
- Risk Manager
- Process Owner
- Task Owner
- Content Controller
- Content Manager
- Risk Assessor

Default User Role mapped for every Internal User Added

RISK MODULE

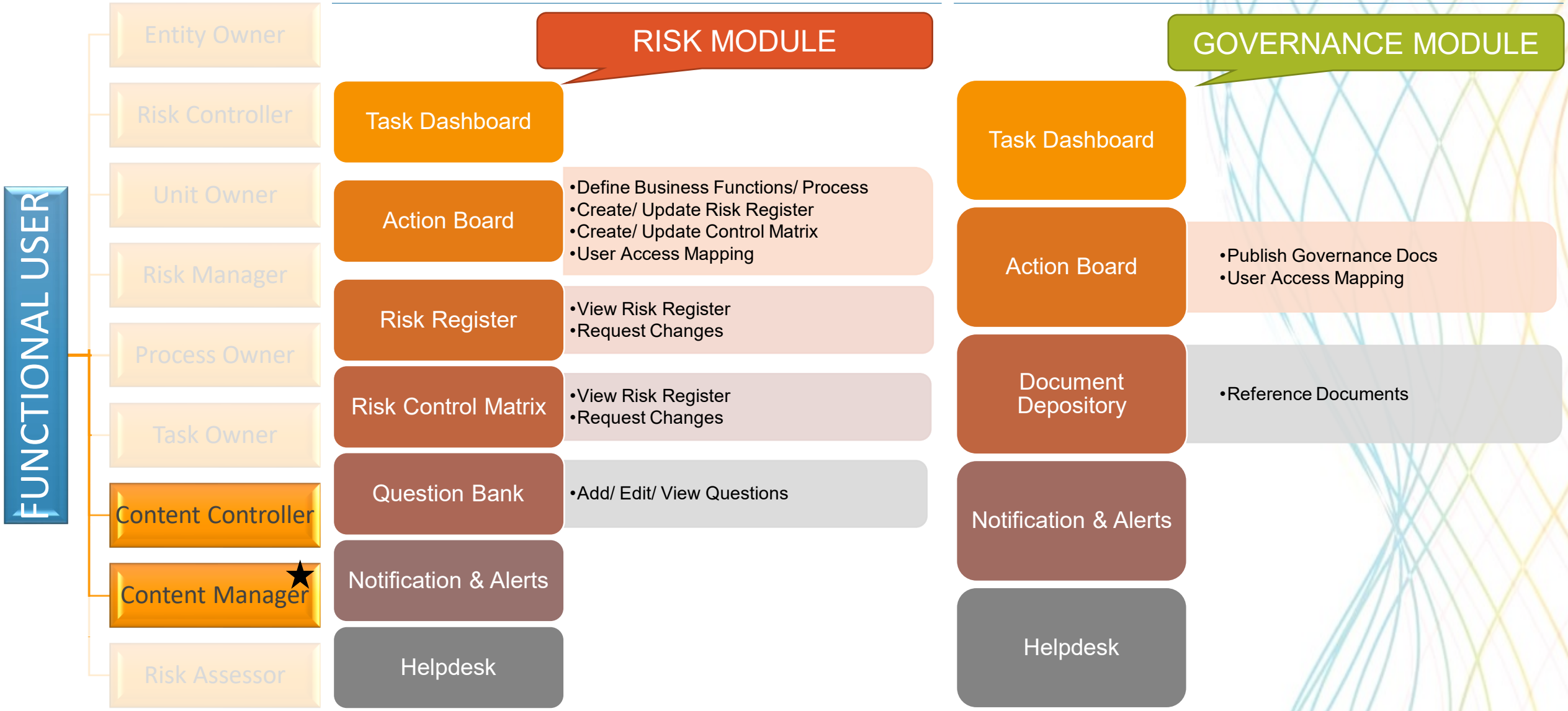
- Task Dashboard
- Action Board
  - •Tasks Scheduled
  - •Manage Tasks
- Assessment Archives
- Notification & Alerts
- Helpdesk

GOVERNANCE MODULE

- Task Dashboard
- Action Board
  - •Assessment Scheduled
  - •Manage Assessment
  - •Assessment Result
- Governance Performance Metric
- Governance Docs Listing
  - •Acknowledgement Requested
- Assessment Archives
- Notification & Alerts
- Helpdesk

** This process flow is indicative only. Please expect changes after project study is complete*

Overview of Process Flow* of User Interface in GRMA



★ Example of additional User roles

* *This process flow is indicative only. Please expect changes after project study is complete*

Overview of Process Flow* of User Interface in GRMA

FUNCTIONAL USER

- Entity Owner
- Risk Controller
- Unit Owner
- Risk Manager
- Process Owner
- Task Owner
- Content Controller
- Content Manager
- Risk Assessor

RISK MODULE

Task Dashboard	
Action Board	•Schedule Internal Assessment •Schedule External Assessment •Manage Assessment •Assessment Result & Monitoring
Risk Performance Metric	•Overall Performance •Impact of KRI's
Risk Register	•View Risk Register •Request Changes
Risk Control Matrix	•View Risk Register •Request Changes
Question Bank	•Add/ Edit/ View Questions
Assessment Archives	
Notification & Alerts	
Helpdesk	

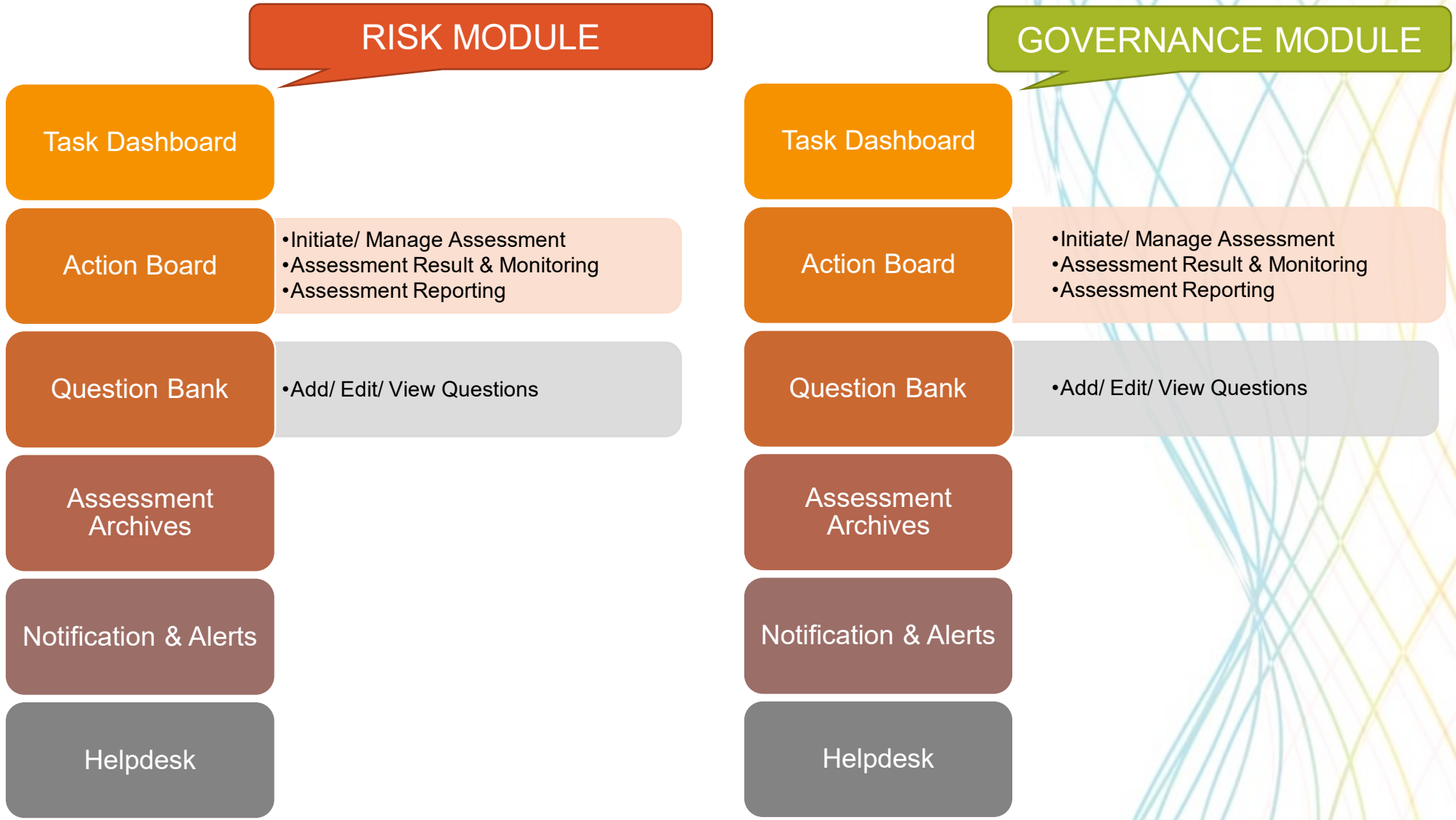
GOVERNANCE MODULE

Task Dashboard	
Action Board	•Schedule Internal Assessment •Schedule External Assessment •Manage Assessment •Assessment Result & Monitoring
Governance Performance Metric	
Question Bank	•Add/ Edit / View Questions
Assessment Archives	
Notification & Alerts	
Helpdesk	

* This process flow is indicative only. Please expect changes after project study is complete

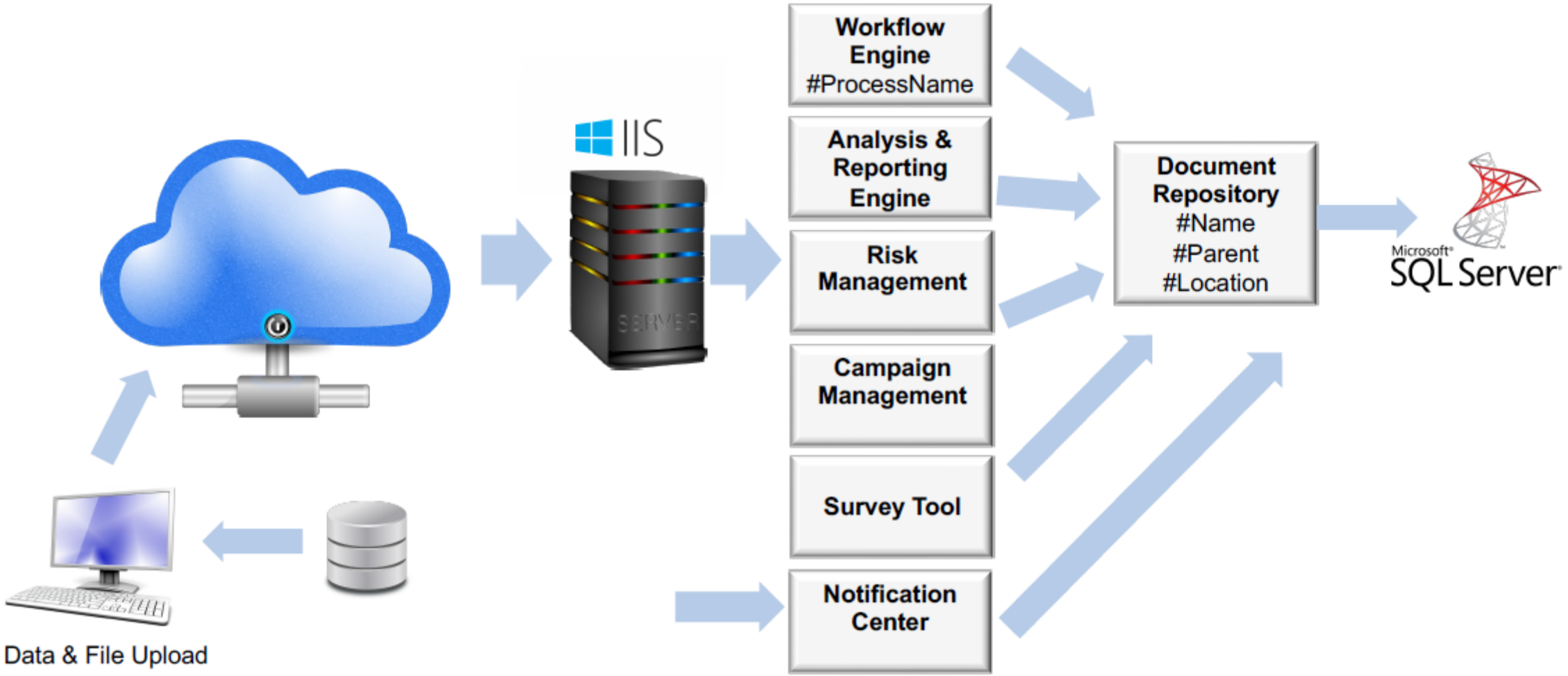
Overview of Process Flow* of User Interface in GRMA

3rd PARTY



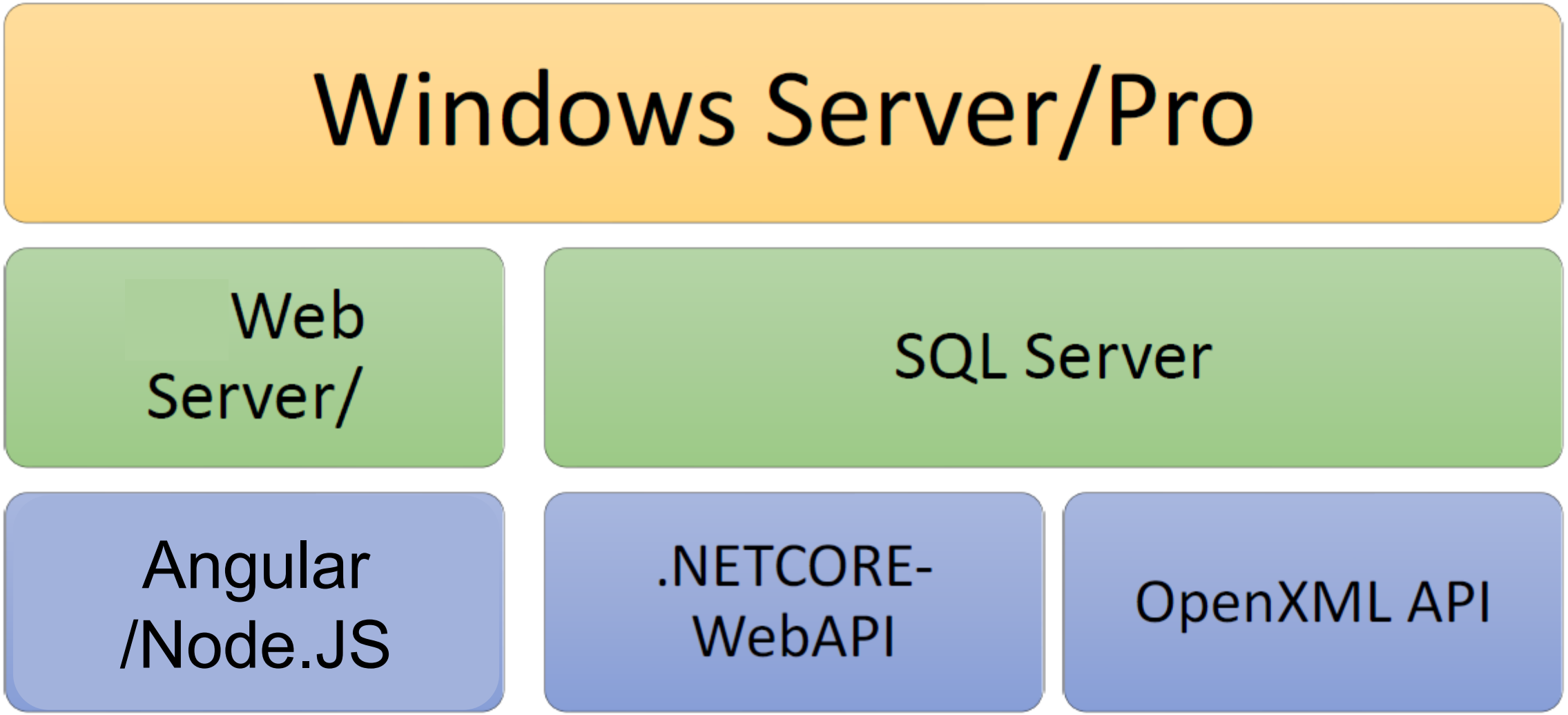
* This process flow is indicative only. Please expect changes after project study is complete

Proposed App Architecture* for GRMA



* This process flow is indicative only. Please expect changes after project study is complete

Proposed Backend Technology for GRMA



* This process flow is indicative only. Please expect changes after project study is complete

ProBuds
Strategy Consulting
Consulting | Compliance | Risk | Management

info@probuds.co.in
+91 98189 46669
+91 99719 83008
NCR-Delhi

For more details, visit:
www.probuds.co