Rest Assured Cyber Security Final Report

University of Toronto: Cyber Security Program Design Final Report

Team 1

Agenda

1. Louisa Define your approach in developing the cybersecurity program

2- Louisa Make assumptions if required and document your assumptions (e.g. assumptions about existing processes, infrastructure and technologies and how they operate)

3- Consider defining and discussing the following components of the designed program:

a. Crown jewels, risks, and threats faced by the target organization

b. Framework you are going to adopt and the domains you are planning to include in the framework

c. The program architecture, governance structure and processes (including the proposed PSGs)

d. Proposed infrastructure components, controls and countermeasures (technology and process-based controls)

e. Current state assessment, roadmap and initiatives to move to a more mature state

f. Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), related metrics and reporting mechanisms

g. Resourcing and the proposed approach for implementing the initiatives 3206 Cyber Security Program Design

Overview of Rest Assured Enterprises

Rest Assured

Introduction to Rest Assured: A Brief Overview

Rest Assured Company Profile

Objectives of Rest Assured's Cyber Security Program

Implement Rest Assured's Cyber Security Strategy

Our Report Approach and Journey

Mobilization
Collect and review documentation, confirm stakeholders, schedule key team meetings and tailor NIST's CSF 2.0, and NIST SP800-207 (Zero Trust Architecture (ZTA) approach to cybersecurity). accelerators, to company's requirements

Outputs: **Kick Off Meeting, Documentation Review; Stakeholder Engagement Plan**

Current State Validation
Conduct stakeholder interviews & focus groups to assess and summarize current state Cyber Security landscape

Outputs: **Determine Approach to Assessment**

Deliverable: **Current State Findings**

Target State Definition
Define target state and reconcile on the Governance approach and strengthening data center controls, integrating cybersecurity into Rest Assured operations, and preparing for the cloud migration with enhanced security measures. based on Rest Assured's company policies and directives, NIST CSF, and NIST SP800-207.

Output: **Cyber Security Governance || NIST Policy-Frameworks**

Deliverable: **Target State Definition**

Maturity & Fit/Gap Analysis
Conduct Fit/Gap analysis to identify areas of lagging maturity referencing the NIST Cyber Security Framework (CSF) 2.0, NIST SP800-207 and develop a maturity and readiness assessment

Outputs: **Workshop #2, Fit/Gap Analysis**

Deliverable: **Maturity & Readiness Assessment**

We are here

Roadmap Development
Develop roadmap and propose catalogue of initiatives to address critical gaps. Identify and integrate in-flight and planned initiatives within proposed roadmap

Output:
Phase 1: Strengthen Data Center Controls (Q1-Q2)
Phase 2: Integrate Cybersecurity into Service Desk Operations (Q3-Q4)
Phase 3: Prepare for Cloud Migration with Enhanced Security Measures (Q1-Q2)
Phase 4: Continuous Monitoring and Optimization (Ongoing)

Deliverable: **Cyber Security Roadmap**

Final Report
Develop final report, and supporting power-point and executive summary to support internal socialization

Output: **Team/Executive Read-Out**

Deliverable: **Final Report**

ASSUMPTIONS

INFRASTRUCUTE ||TECNOLOGY

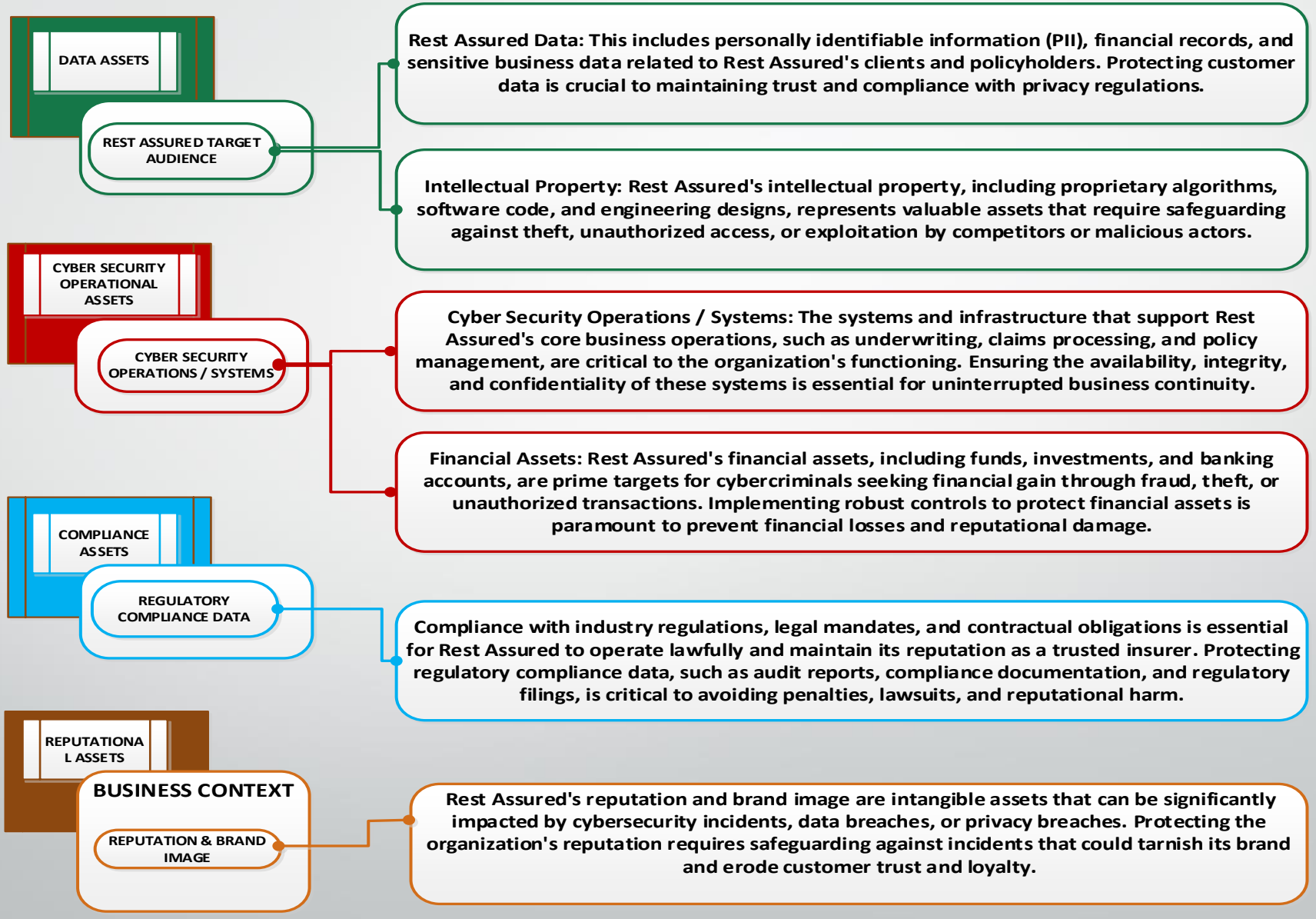
Ref#	Rest Assured Infrastructure – Technology (IT Assumptions	Impact
IT-ASM1	Assumption: Legacy systems within Rest Assured's infrastructure may have outdated software and firmware, making them susceptible to known vulnerabilities.	Impact: Outdated software and firmware pose a significant security risk as they may contain unpatched vulnerabilities that threat actors can exploit to gain unauthorized access or disrupt operations.
IT-ASM2	Assumption: Limited visibility and control over endpoint devices, including mobile devices used by employees, may expose Rest Assured to increased risk of data loss or compromise.	Impact: Without adequate endpoint security measures, such as mobile device management solutions and endpoint detection and response capabilities, Rest Assured may struggle to detect and mitigate threats targeting endpoint devices, leading to potential data breaches and security incidents.
IT-ASM3	Assumption: Inadequate logging and monitoring capabilities across infrastructure and applications may hinder timely detection and response to security incidents.	Impact: Without comprehensive logging and monitoring, Rest Assured may struggle to identify malicious activities or anomalies indicative of a security breach, prolonging the time to detect and respond to incidents and increasing the potential impact of cyberattacks.
IT-ASM4	Assumption: Lack of regular security assessments and audits may result in unidentified vulnerabilities and weaknesses in Rest Assured's systems and processes.	Impact: Without periodic security assessments and audits, Rest Assured may remain unaware of existing security gaps and vulnerabilities, leaving the organization susceptible to cyber threats and regulatory non-compliance.
IT-ASM5	Assumption: Legacy systems within Rest Assured's infrastructure may have outdated software and firmware, making them susceptible to known vulnerabilities.	Impact: Outdated software and firmware pose a significant security risk as they may contain unpatched vulnerabilities that threat actors can exploit to gain unauthorized access or disrupt operations.

Cont..... ASSUMPTIONS OPERATIONAL

Ref#	Rest Assured Infrastructure – Operational (O) Assumptions	Impact
O-ASM1	Assume that the current MSSP lacks adequate visibility and responsiveness to emerging threats.	Impact: Increased risk of undetected or delayed response to cyber threats, potentially leading to data breaches or other security incidents.
O-ASM2	Assume that there is limited integration between the IT service desk operations and cybersecurity functions.	Impact: Lack of coordination and communication between IT support and cybersecurity teams may result in slower incident response times, ineffective troubleshooting, and increased vulnerability to cyber attacks.
O-ASM3	Budget Allocated for Cyber Security Initiatives	Impact: The budget adjustment may impact the scope and timeline of cybersecurity initiatives, potentially delaying critical security improvements or leaving gaps in protection.
O-ASM4	Sarbanes and Oxley (SOX) Act assuming the company is publicly traded; PCI-likely debit/credit card information involved; GDPR: since it looks like there are customers in Europe (worldwide company)	Impact: Non-compliance with regulatory requirements may result in legal consequences, fines, reputational damage, and loss of customer trust. It may also indicate weaknesses in data protection and governance practices.
O-ASM5	Assume that there is limited user awareness and training regarding cybersecurity best practices.	Impact: Increased susceptibility to social engineering attacks, phishing attempts, and other forms of user-related security breaches. Users may inadvertently compromise security through actions like clicking on malicious links or sharing sensitive information.
O-ASM6	Assume that there are vulnerabilities in legacy systems or applications due to outdated software or lack of patching.	Impact: Heightened risk of exploitation by cyber attackers targeting known vulnerabilities, potentially leading to unauthorized access, data breaches, or service disruptions.
O-ASM7	Assume that there may be insider threats or malicious activities from disgruntled employees or contractors.	Impact: Heightened risk of exploitation by cyber attackers targeting known vulnerabilities, potentially leading to unauthorized access, data breaches, or service disruptions.
O-ASM8	Assume that there is a lack of formal incident response plan or procedures in place.	Impact: Ineffective response to security incidents, prolonged downtime, and increased damage from cyber attacks. Without a structured plan, the organization may struggle to contain and mitigate the impact of security breaches.
O-ASM9	Assume that there may be compliance gaps in other regulatory frameworks apart from SOX, PCI, and GDPR, depending on the industry and geographical locations of operation.	Impact: Similar to non-compliance with SOX, PCI, and GDPR, failure to meet other regulatory requirements may lead to legal penalties, loss of business opportunities, and damage to the organization's reputation.
O-ASM10	Assume that there may be challenges in ensuring the security of third-party vendors and supply chain partners.	Impact: Increased risk of supply chain attacks, data breaches, or other security incidents originating from vulnerabilities in third-party systems or services. This can result in financial losses, regulatory scrutiny, and damage to customer trust.

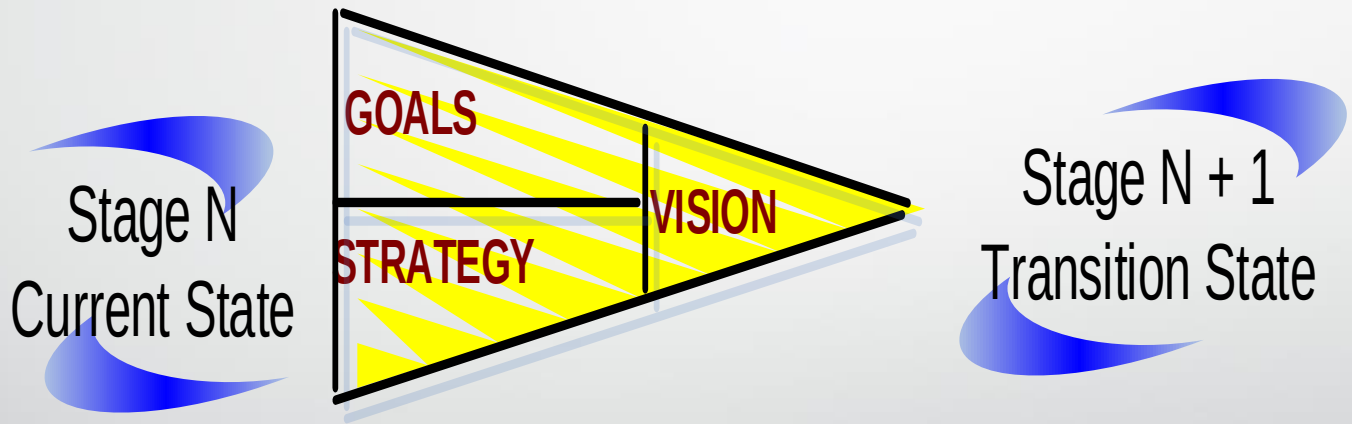
- a. **Crown jewels**, risks, and threats faced by the target organization

Crown Jewels



- a. Crown jewels, **risks**, and threats faced by the target organization

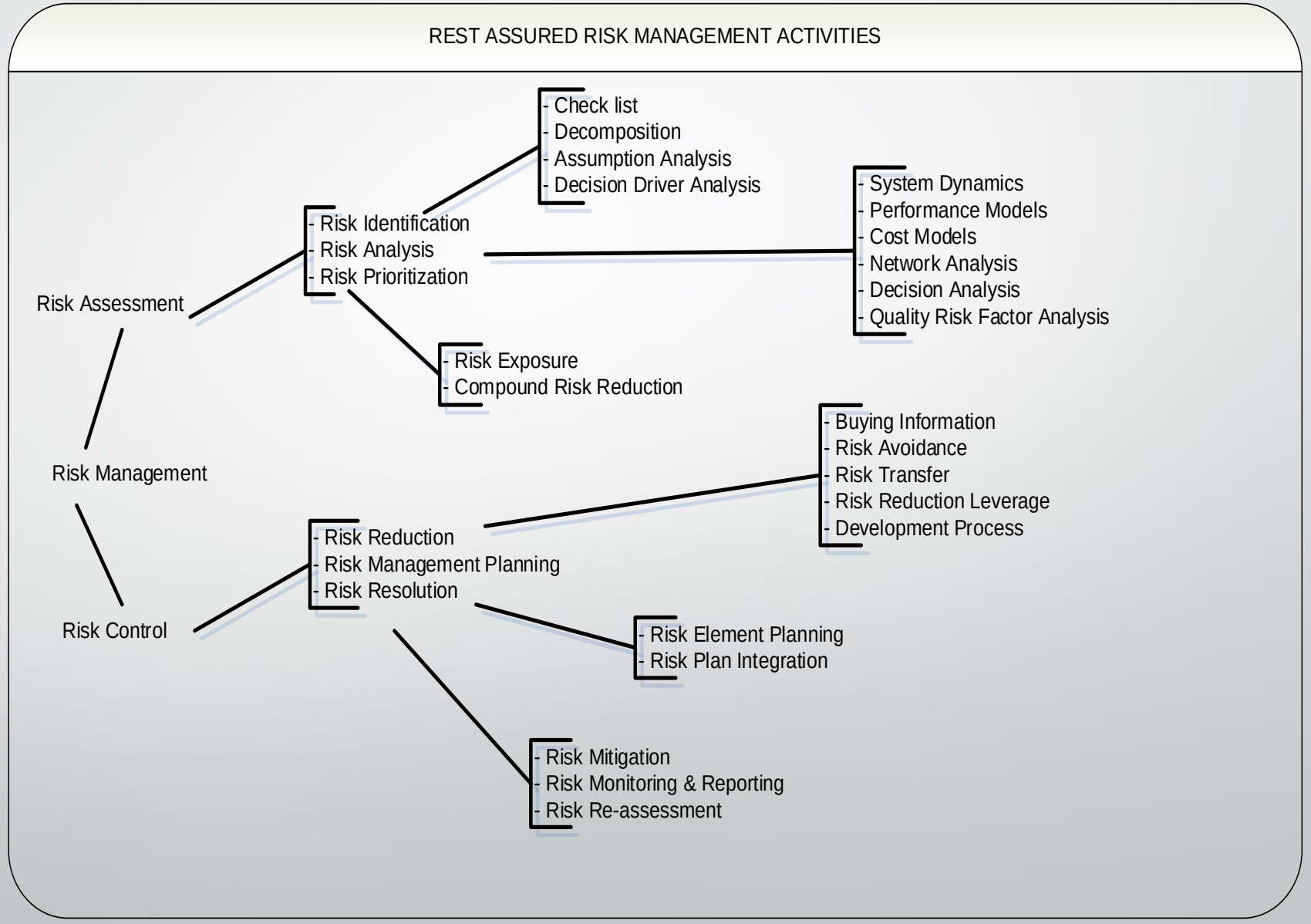
REST ASSURANCE CLOUD RISK MANAGEMENT MAP ARCHITECTURE



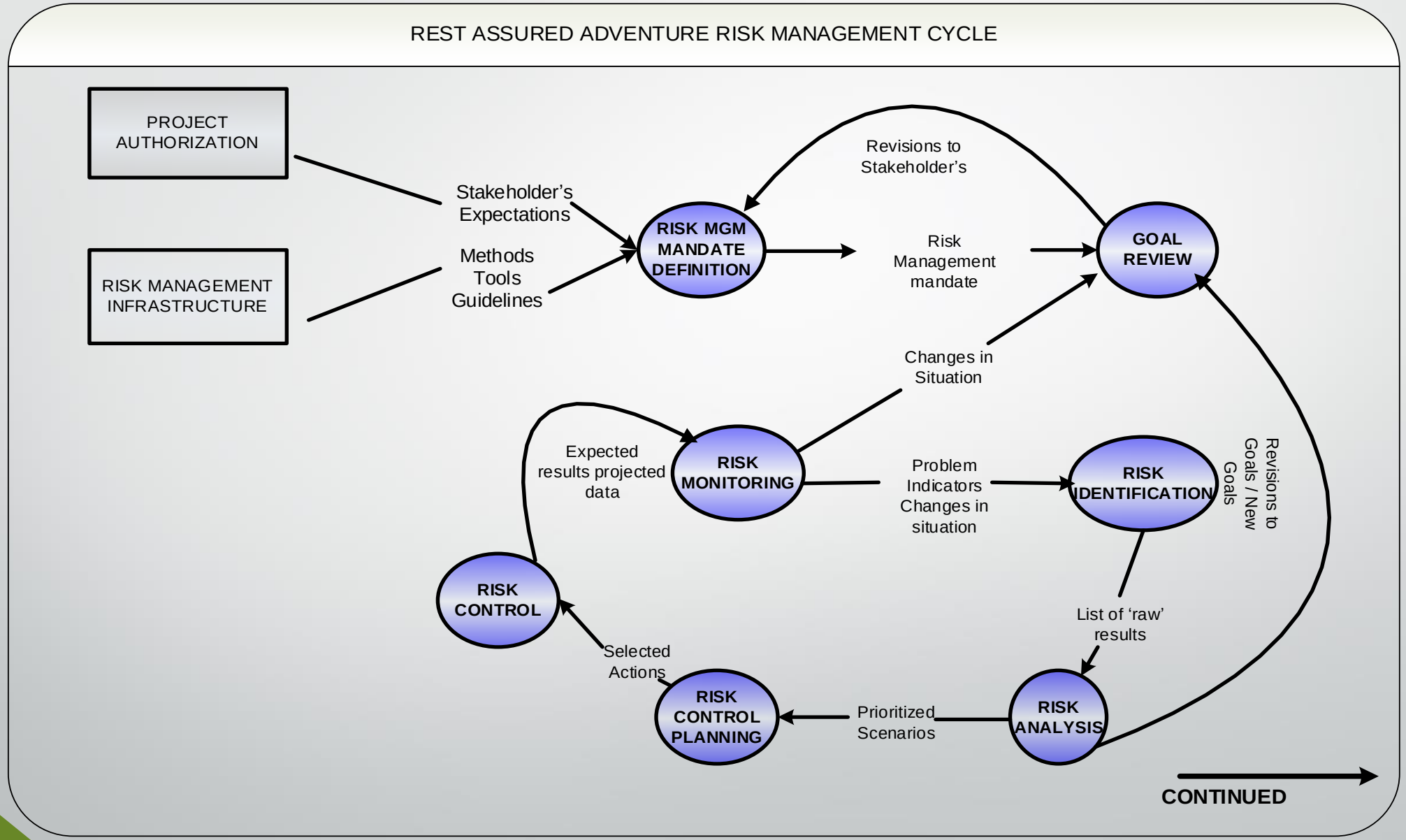
Key Risks & Threats Planned Risk Mitigation Strategy

Key Risks & Threats

Data Breaches: Unauthorized access to customer data or financial information could lead to reputational damage, regulatory penalties, and financial losses.
Insider Threats: Malicious or negligent employees with access to sensitive information pose a significant risk of data theft or sabotage.
Cyberattacks: Threat actors may target Rest Assured's infrastructure and applications through methods such as ransomware, phishing, or DDoS attacks.
Third-Party Risks: Dependence on third-party vendors, including the MSSP, increases the risk of supply chain attacks or data breaches.
Regulatory Compliance: Failure to comply with data protection regulations such as GDPR or industry standards like PCI DSS could result in legal consequences and fines.
Social Engineering: Threat actors may attempt to manipulate individuals within Rest Assured to divulge sensitive information or perform unauthorized actions.
Zero-Day Exploits: Vulnerabilities in software or systems that are unknown to the vendor or have not yet been patched could be exploited by attackers.
Supply Chain Risks: Risks associated with third-party suppliers or service providers, including software vulnerabilities, data breaches, or compliance issues.



- a. Crown jewels, **risks**, and threats faced by the target organization



- a. Crown jewels, **risks**, and threats faced by the target organization

REST ASSURED OVERVIEWS OF OUTPUTS & EXIT CRITERIA OF RISK PROCESS

Risk Process	Description	Output
Risk Management Mandate definition	Define the scope and frequency of risk management. Recognize all relevant stakeholders	Risk Management mandate; why, what, when, who, how, and for whom
Goal Review	Review the stated goals for the project, refine them and define implicit goals and constraints explicitly. Analyze stakeholders association with the goals	Explicit goal definitions
Risk Identification	Identify potential threats to the project using multiple approaches	A list of 'raw' risks
Risk analysis	Classify and consolidate risks. Complete Risk scenarios for main risk events. Estimate risk effects for all risk scenarios. Estimate probabilities and utility loses of risk scenarios	Completed Risk Process analysis graphs for all analyzed risks Ranked risk scenarios
Risk Control Planning	Select the most important risks for risk control planning. Propose Risk controlling actions for the most important tasks. Select the risk controlling actions to be implemented.	Selected risk controlling actions
Risk Control	Implement the risk controlling actions	Reduced Risks
Risk Monitoring	Monitor the risk situation	Risk status information

COBIT COMPONENTS OF REST ASSURED's GOVERNANCE SYSTEM

Rest Assured Executive Bboard should ensure that structures and practices exist and are well-governed so that it receives timely, complete, relevant, accurate and reliable information to perform its oversight effectively

Ensuring that all Rest Assured employees receive adequate training

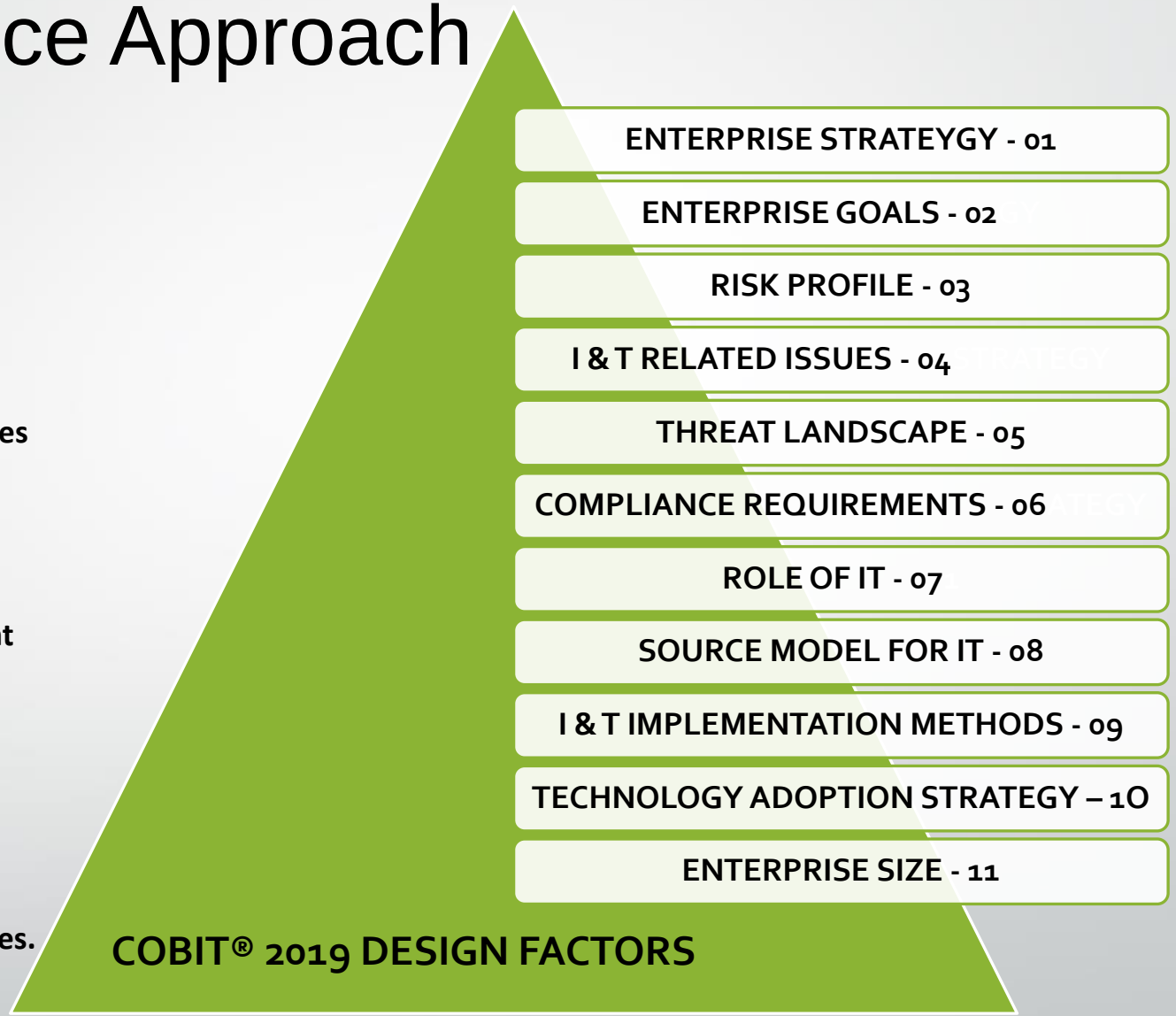
Rest Assured board should ensure that the culture of the organization is healthy, regularly monitored and evaluate the Company's core culture and values, assess the integrity and ethics of senior management, and as needed, intervene to correct misalign corporate objectives and culture for the Cyber Security Program.

Ref: www.businessbeam.com

Governance Approach

Outcomes

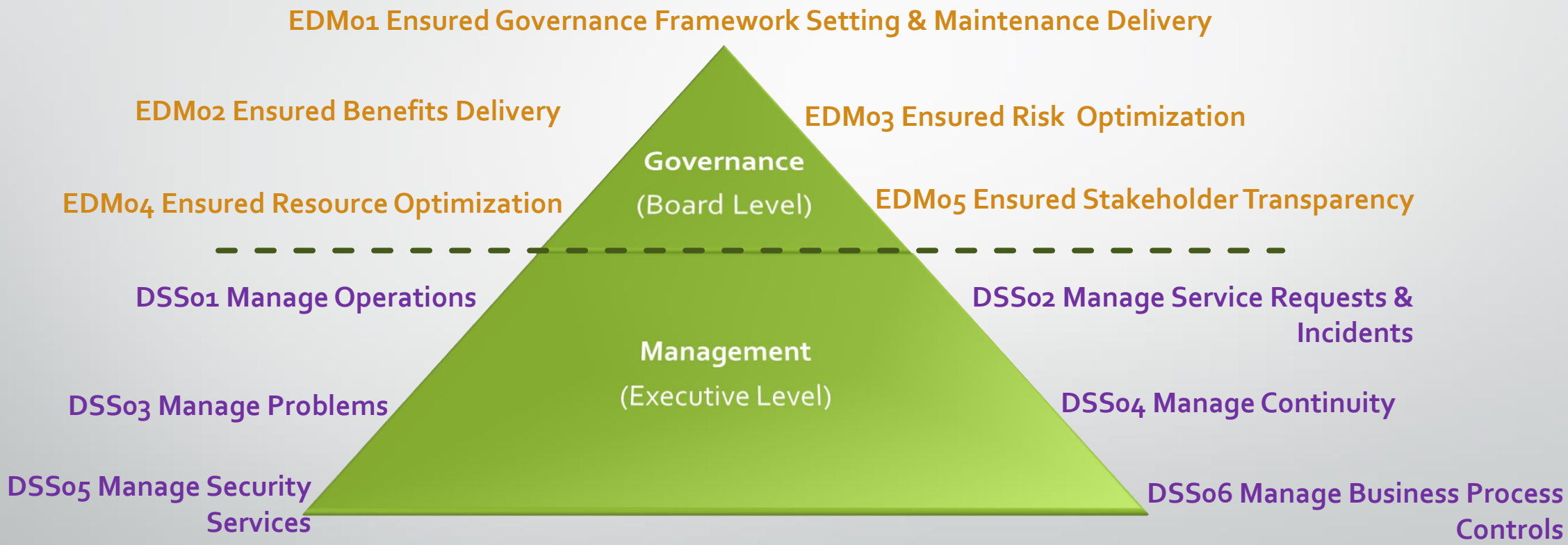
- Enhance security controls and monitoring mechanisms within the data center environment.
- Ensure compliance with industry standards and regulatory requirements.
- Improve incident detection and response capabilities through integration with service desk operations.
- Enhance user awareness and incident reporting mechanisms.
- Ensure a secure transition to the cloud environment with enhanced security measures.
- Mitigate risks associated with cloud migration and adoption.
- Continuously monitor and optimize cybersecurity controls and processes across the organization.
- Adapt to evolving threats and emerging technologies.



Ref: ISACA *COBIT® 2019 Design Guide: Designing an Information & Technology Governance Solution – figure 2.4, USA*

Governance Framework

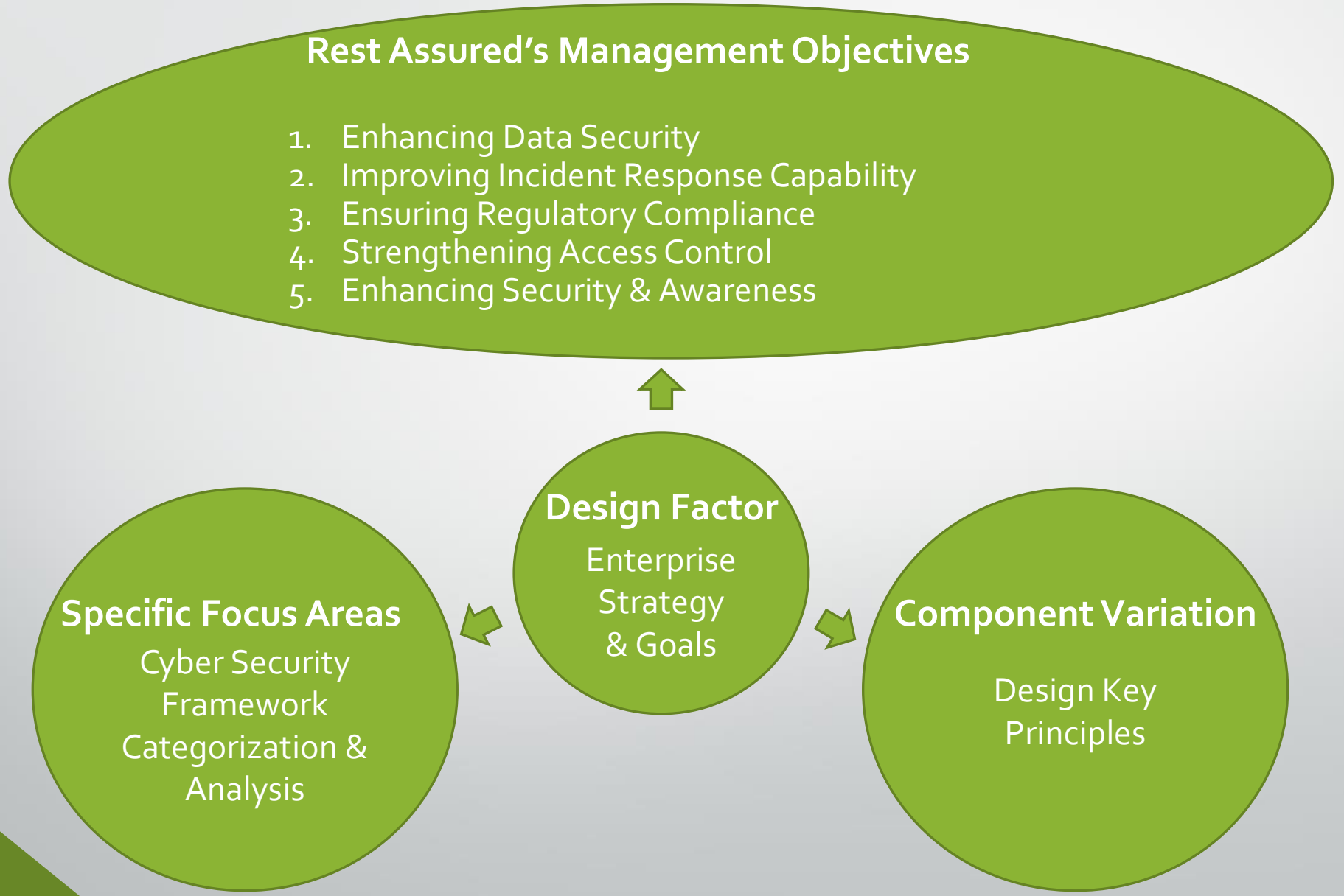
- The Control Objectives for Information and Related Technology (COBIT) 2019 is the most widely use IT governance and management framework, providing a common language for all Rest Assured stakeholders to help with compliance, risks and auditing.



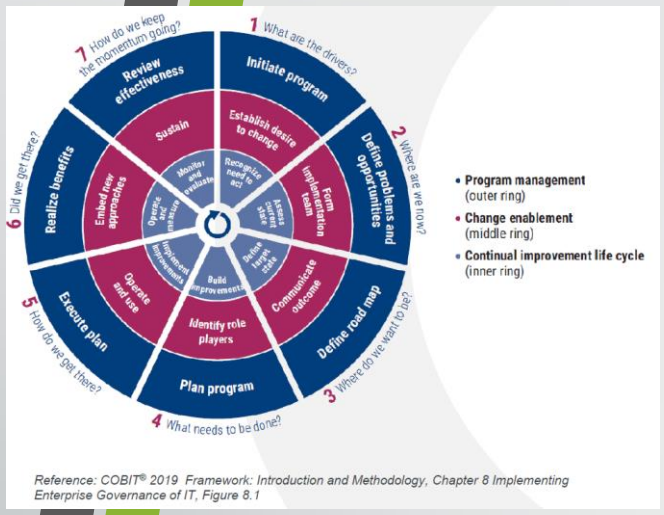
Ref: Getting to know COBIT 2019 (yhbcpa.com)

LEGEND: Evaluate, Direct & Monitor (EDM)
Deliver, Service & Support (DSS)

Governance Tailoring



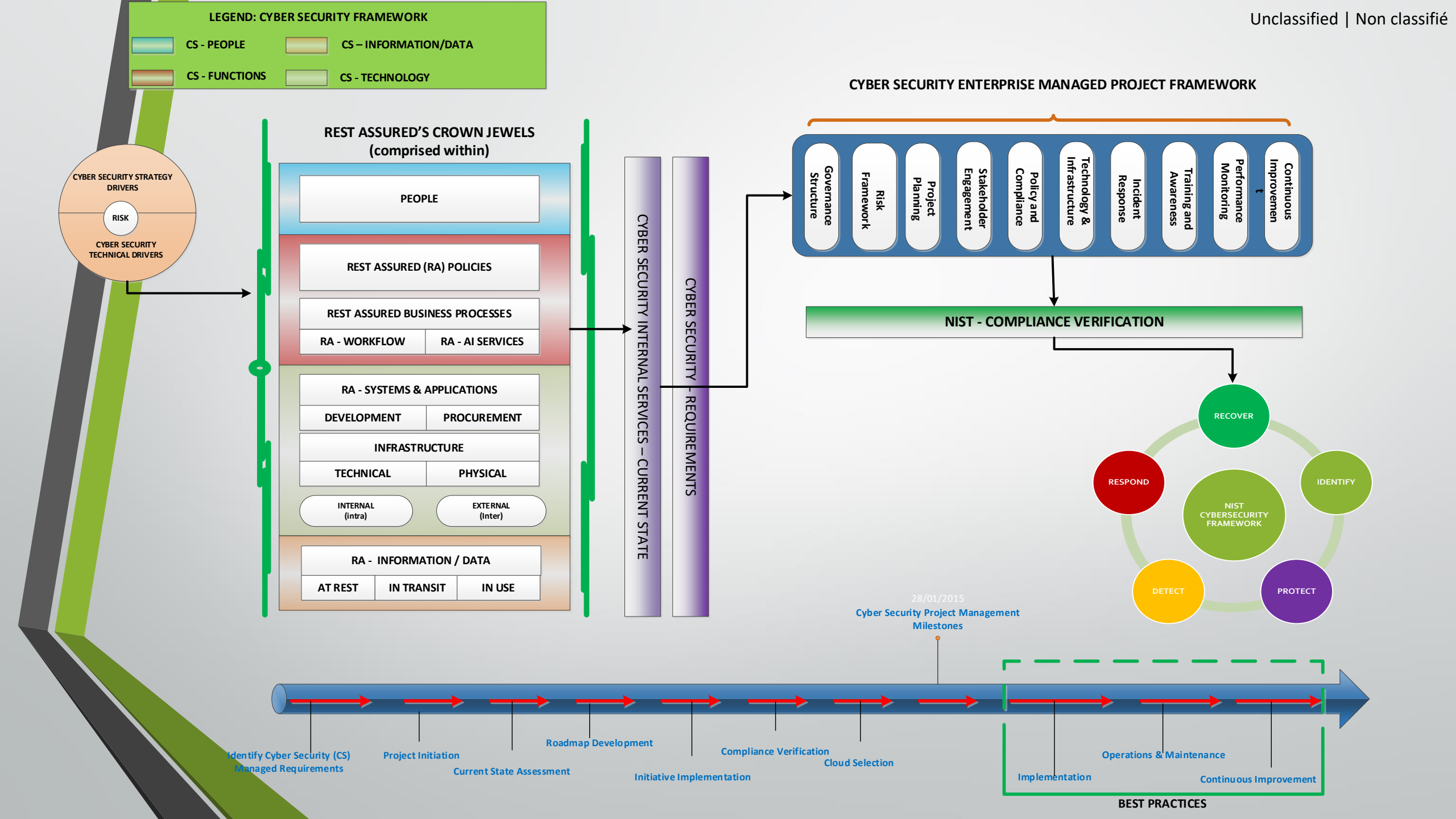
Governance Tailoring



Reference: COBIT® 2019 Framework: Introduction and Methodology, Chapter 8 Implementing Enterprise Governance of IT, Figure 8.1

COBIT 2019 Continuous Improvement Toolkit

		Program Management	Change Management	Continual improvement life cycle
1	What are the drivers?	Initiate program	Establish desire to change	Recognize the need to act
2	Where are we now?	Define problems and opportunities	Form the implementation team	Assess current state
3	Where do we want to be?	Define roadmap	Communicate outcome	Define target state
4	What needs to be done?	Plan program	Identify role players	Build improvements
5	How to we get there	Execute plan	Operate and use	Implement improvements
6	Did we get there?	Realize benefits	Embedded new approaches	Operate and measure
7	How do we keep the momentum going?	Review effectiveness	Sustain	Monitor and evaluate


LEGEND: CYBER SECURITY FRAMEWORK
CS - PEOPLE
CS – INFORMATION/DATA
CS - FUNCTIONS
CS - TECHNOLOGY
CYBER SECURITY STRATEGY DRIVERS
RISK
CYBER SECURITY TECHNICAL DRIVERS
REST ASSURED'S CROWN JEWELS (comprised within)
PEOPLE
REST ASSURED (RA) POLICIES
REST ASSURED BUSINESS PROCESSES
RA - WORKFLOW
RA - AI SERVICES
RA - SYSTEMS & APPLICATIONS
DEVELOPMENT
PROCUREMENT
INFRASTRUCTURE
TECHNICAL
PHYSICAL
INTERNAL (intra)
EXTERNAL (Inter)
RA - INFORMATION / DATA
AT REST
IN TRANSIT
IN USE
CYBER SECURITY INTERNAL SERVICES – CURRENT STATE
CYBER SECURITY – REQUIREMENTS
CYBER SECURITY ENTERPRISE MANAGED PROJECT FRAMEWORK
Governance Structure
Risk Framework
Project Planning
Stakeholder Engagement
Policy and Compliance
Technology & Infrastructure
Incident Response
Training and Awareness
Performance Monitoring
Continuous Improvement
NIST - COMPLIANCE VERIFICATION
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
NIST CYBERSECURITY FRAMEWORK
28/01/2015
Cyber Security Project Management Milestones
Identify Cyber Security (CS) Managed Requirements
Project Initiation
Current State Assessment
Roadmap Development
Initiative Implementation
Compliance Verification
Cloud Selection
Implementation
Operations & Maintenance
Continuous Improvement
BEST PRACTICES

Rest Assured's Cyber Security Strategic Service Initiatives Roadmap

DRAFT

An approach to cyber security that is based on constant verification (zero trust), where users can seamlessly and securely access the tools, they need thru a single secure digital identity.

- Preform a current state evaluation of existing Rest Assured's cyber security landscape
- Prioritize initiatives to achieve the target state and to strengthen cybersecurity resilience across the Rest Assured global / regional footprint, to prepare for, respond to and recover from attacks.

Cyber Security - Zero Trust Architecture

Infrastructure

ICAM

Service Desk

Enabling

GAPS

- Insufficient endpoint visibility, detection, protection and response.
- Inconsistent access control for privileged accounts across the Rest Assured environments.
- Lack of an Enterprise Multi-Factor Authentication service.
- Lack of comprehensive Enterprise ICAM service.
- No Enterprise log collection and analysis service (SIEM – CLS)
- No Attack Surface Management solution. Need to evolve vulnerability management to be risk based. Implement CSCA to review controls.

Phase 1: Strengthen Cyber Security Controls (0-6 months)

- G1-Enhance security controls and monitoring mechanisms within the data center environment.
- G2-Ensure compliance with industry standards and regulatory requirements.

Initiative 1: Conduct Security Assessment

Initiative 2: Implement Security Enhancements

Initiative 3: Update incident response plan and conduct tabletop exercises.

Initiative 4: Patch critical vulnerabilities

Initiative 5: Enhance Access Control.

Phase 2: Medium – Term Goals (6-12 Months)

- G3-Improve incident detection and response capabilities through integration with service desk operations.
- G4-Enhance user awareness and incident reporting mechanisms.

Initiative 6: Critical Assets – Network Segmentation:

Initiative 7: Enhance Endpoint Security

Initiative 8: Implement Encryption – Data at Rest / Data in Transit:

Initiative 9: Strengthen vendor risk management processes and controls.

Initiative 10: Deploy a Security Information and Event Management (SIEM) system.

Phase 3: Log Term Strategy (12+ months)

1. Continuous evolution and strengthening of cybersecurity across Rest Assured.

Initiative 11: Develop and implement a formal cybersecurity governance framework.

Initiative 12: Conduct regular security audits and assessments to maintain compliance.

Initiative 13: Implement a comprehensive data loss prevention (DLP) solution..

Initiative 14: Enhance incident response capabilities with automation and orchestration.

Initiative 15: Explore emerging technologies and trends to anticipate future threats.

f. Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), related metrics and reporting mechanisms

Key Risk Indicators	Key Performance Areas
Unauthorized Access Attempts	Zero Trust Adoption Rate
Anomalous User Behavior	Incident Detection and Response Time
Data Exfiltration Attempts	User Authentication Strength
Security Control Violations	Access Control Effectiveness
Vulnerability Exploitation	Data Protection Compliance

Recommendations

Prioritize COBIT 2019 objectives
Formalizing an IT Governance Board
Implement robust security controls and encryption mechanisms across all environments.
Strengthen identity, access management practices, and enforce least privilege principles.
Adapt a security framework tailored to Rest Assured. Also, cybersecurity policies such as an Incident Response policy, Encryption policy and Security policy need to be documented.
Enhance monitoring, auditing, and incident response capabilities to improve threat detection and response.
Document, cybersecurity policies i.e., Incident Response, Encryption, and Security policies.
Conduct regular security assessments, audits, and training programs to address gaps and vulnerabilities
Establish comprehensive business continuity, disaster recovery, and third-party risk management strategies.
Enhance network security, endpoint protection, and data loss prevention measures to mitigate cyber threats effectively.
Ensure compliance with regulatory requirements and industry standards through initiative-taking risk management and governance frameworks.

What We've Learned so far

Technology

- In conclusion, the Rest Assured Cybersecurity Project emphasizes the strategic deployment of advanced technologies to enhance our security posture.
- Through the implementation of state-of-the-art security controls, including multi-factor authentication, encryption, and advanced threat detection, we aim to fortify our defenses against cyber threats.
- By leveraging cutting-edge technologies and continuously monitoring our systems, we can proactively detect and respond to security incidents, safeguarding our critical assets and ensuring the resilience of our infrastructure.

Policy

- Through the development and enforcement of comprehensive security policies, including access control policies, incident response protocols, and data protection guidelines, Rest Assured can establish clear standards for security across the organization.
- Rest Assured policies must be developed to guide establishment of level of trust, govern level of access, and clarify risk tolerance
- Additional legal and contractual agreements governing external collaborators are required to ensure accountability in cases of misuse of access, compromise by malicious actors, etc.
- By promoting a culture of security and compliance, supported by well-defined policies and procedures, Rest Assured can enhance their ability to mitigate risks, address vulnerabilities, and maintain regulatory compliance.

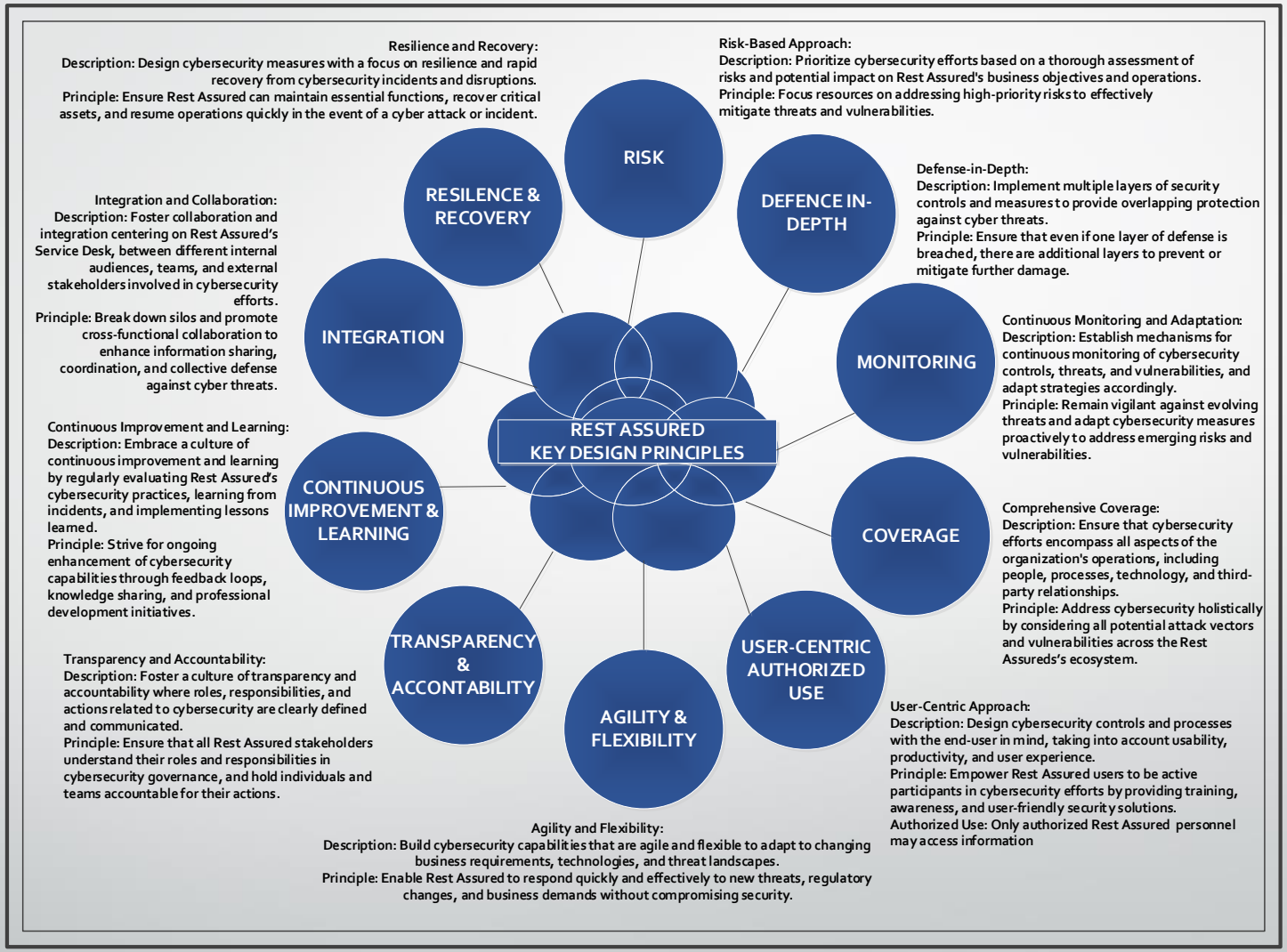
Security

- Rest Assured Cybersecurity Project recognizes the critical importance of applying security in protecting their data assets and ensuring the confidentiality, integrity, and availability of information.
- Through the implementation of security measures, including encryption, access controls, and data loss prevention mechanisms, we strive to safeguard our sensitive data from unauthorized access, disclosure, or tampering.
- By prioritizing data protection and privacy, we demonstrate our commitment to safeguarding customer trust, maintaining regulatory compliance, and preserving the integrity of our organization's operations.

Ask Us Anything

Appendix

Key Design Principles



What Problem is ZTA Trying to Solve?

Enhance Rest Assured's User Experience While Strengthening Security Posture

Collaborate Seamlessly

- Work with anyone, anywhere with trusted organizations*
- Use less devices
- Gain direct access to Rest Assured's computing power, storage, tools and workstations
- Work from a private cloud that is separate from the corporate network for the ZT development

Identity is the Glue

- Centralize management of collaborators and their roles
- Reduce number of credentials and accounts for Rest Assured's Admin's to manage
- Offload authentication to trusted Identity Providers such as ……

Collaborate Securely

- Grant access to applications, files or desktops to users based on who they are and what they do - RBAC
- Rest Assured environments are built with security controls based on its information classification
- Security is seamless to Rest Assured
- All actions are monitored and audited

Zero Trust Model - Modern Security Architecture | Microsoft Security

Zero Trust has become an important cybersecurity issue

Top three cybersecurity priorities

1. Protecting an expanding perimeter
2. Improving user security awareness
3. Adapting to a changing threat landscape

When asked what their organization's top cybersecurity priorities were for the next 12 months, at the top of the list was a big Zero Trust issue: **protecting an expanding perimeter** (due to cloud adoption, remote work, global workforce, etc.).

Ref: zero-trust-implementation-in.pdf (entrust.com)

Rest Assured's Zero Trust Architecture Proposed Journey Map

PoC 1 Identity-Aware

FY 2024

Where We should start

- Built a cloud sandbox and tested an open source and non-commercial ready offering with Rest Assured

What We Learned

- ZTA relies on a strong identity foundation based on common, cohesive identity
- Rest Assured has many identity repositories that would require synchronization to be positioned for ZTA

PoC 2 External Collaboration

FY 2024

Exploring External Collaboration

- Following Rest Assured ICAM concepts expand scope to develop a mock-up for external collaborators

In-Scope Capabilities

- Collaborator Identity Repository
- Collaborator Web Access Broker
- Collaborator Mock-up Identity Provider (IDP)
- Collaborator Identity Governance and Administration (IGA)

PoC 3 TBD

FY 2025

Explore What Is Needed Next

- Securely deploy three-tier application in hybrid cloud environment
- Implement non-repudiation and API security using a chosen Framework
- Build on ICAM capabilities achieved in PoC 2 (e.g., Verifiable Credentials)
- Implement proactive Monitoring and Alerting
- Device authentication

Key Takeaway: Rest Assured will initiate in its first year a ZTA PoC with a focus on partners. Our goal is to demonstrate how Rest Assured can implement ZTA capabilities