Password write. Welcome Mr.
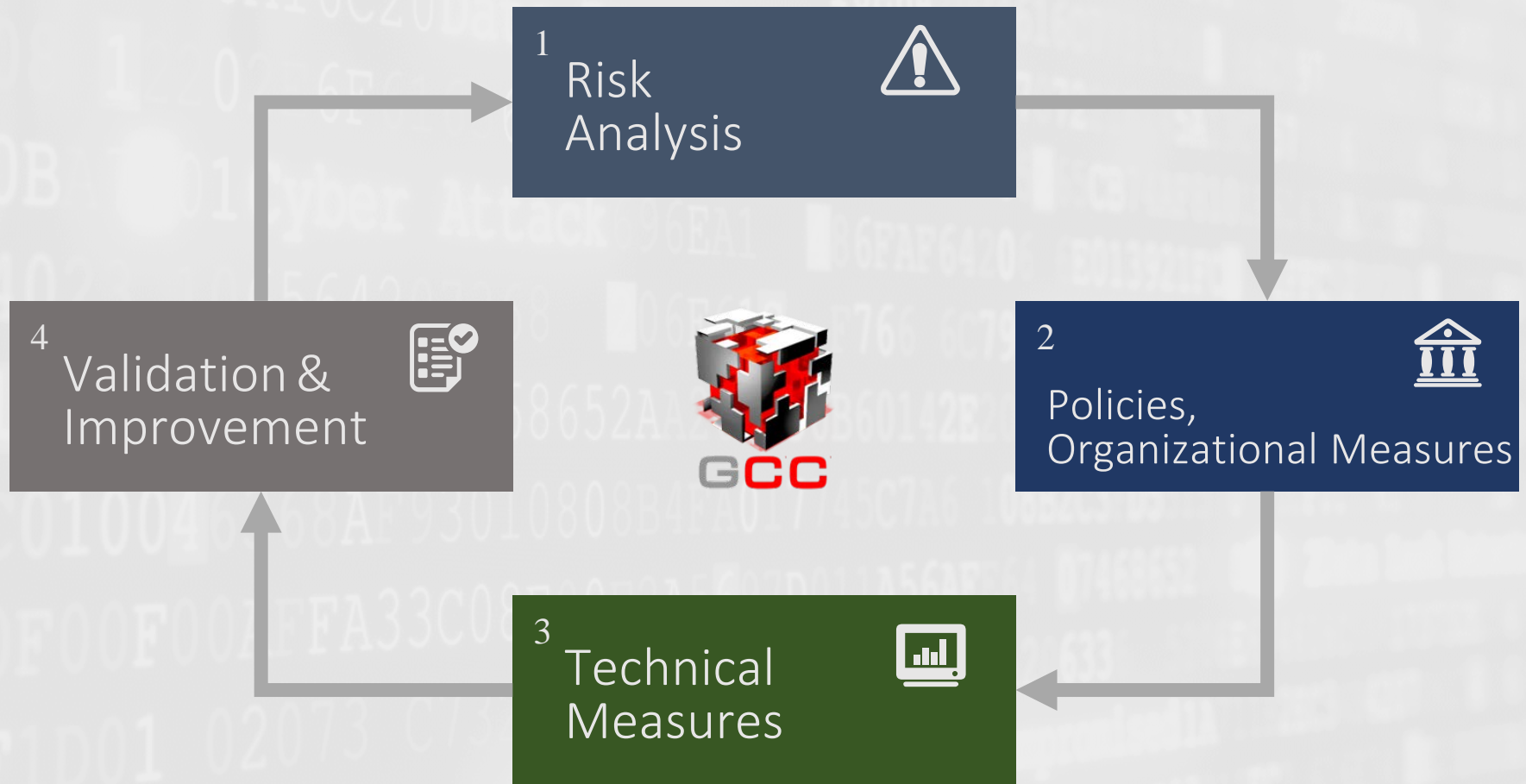
GCC

THE BASIC GCC RISK FRAMEWORK

1 Risk Analysis ⚠️

2 Policies, Organizational Measures 🏛️

3 Technical Measures 📊

4 Validation & Improvement 📋✓

GCC

CYBER RISK ANALYSIS

What is our plan to respond to a data breach?

Are we adequately insured?

How do we monitor our systems and prevent breaches?

Do our security goals align with business priorities?

CYBERSECURITY CHECKLIST

How much is the issue of security integrated into your business?

How often do we verify the effectiveness of our security?

Can you answer these questions about your business?

Are we compliant with industry regulatory requirements?

Do we have the basic rights for security measures?

Have we evaluated our third-parties with access to sensitive information?

Have we identified and protected our most valuable processes and information?

Do we treat cybersecurity as a business or an IT responsibility?

GCC

WHERE DOES YOUR SECURITY STAND?

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Continuous Monitoring	Communication	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Maintenance		Mitigation	
Risk Management Strategy	Info. Protection Processes & Procedures		Improvements	
	Protective Technology			

GCC

THE GCC BASIC CHECKLIST

Cybersecurity Questions for Your Business

Do we treat cybersecurity as a business or IT responsibility?

Do our security goals align with business priorities?

Have we identified and protected our most valuable processes and information?

Does our business culture support a secure cyber environment?

Do we focus on security compliance or security capability?

Are we certain our third-party partners are securing our most valuable information?

Do we regularly evaluate the effectiveness of our security?

Do we have a plan for responding to a security breach?

GCC

THE GCC BASIC CHECKLIST

Cybersecurity Questions for Your Business

Are the Internet services that are being accessed and used safe?

Are employees trained for cyber attacks?

Are mobile devices such as laptops, smartphones and tablets protected from a data breach?

Is a cyber attack from outside the corporate network possible? What are your external access options?

Are there any contingency strategies and exercises?

Are there periodic updates for operating systems and programs

Do you know the email sender who is requesting data?

Do I trust the source of the links/ download?

IS YOUR ORGANIZATION PREPARED?

BE PREPARED
- Ongoing Monitoring
- Defined Planning & Testing
- Prepared Incident Response
- Cyber Insurance

SECURITY THROUGH
PROTECTION & RESILIENCE

SET THE BAR
- Establish a Risk-Based Strategy aligned with Business Strategy
- Identify Most Valuable Assets & Security Measures to Protect
- Align IT Architecture with Capability

SECURITY THROUGH
STRATEGY & ALIGNMENT

GET THE BASICS RIGHT
- Set Access Protocols
- Conduct Regular Patching & Vulnerability Protocols
- Secure Critical Systems
- Conduct Regular Testing & Root-Cause Analysis

SECURITY THROUGH
CONTROL

PERSONAL PROTECTION
- Develop Security Awareness
- Security Culture Drive from Top
- Identify Consequences of Poor Security

SECURITY THROUGH
BEHAVIOR

GCC

CONTACT US FOR A FREE ASSESSMENT

info@globalcyberconsultants.com

Security Assessments

Technical Due Diligence

Global compliance

GCC

Software Procurement Services

Employee Cyber Training

Information Security Policies