CATALYST

# Governance, Risk, Compliance & Security (“GRCS”)

March 2023

Grady Kidder, Carson Bliss, Killian Bubrosky

# Defining the Convergence of GRC & Security

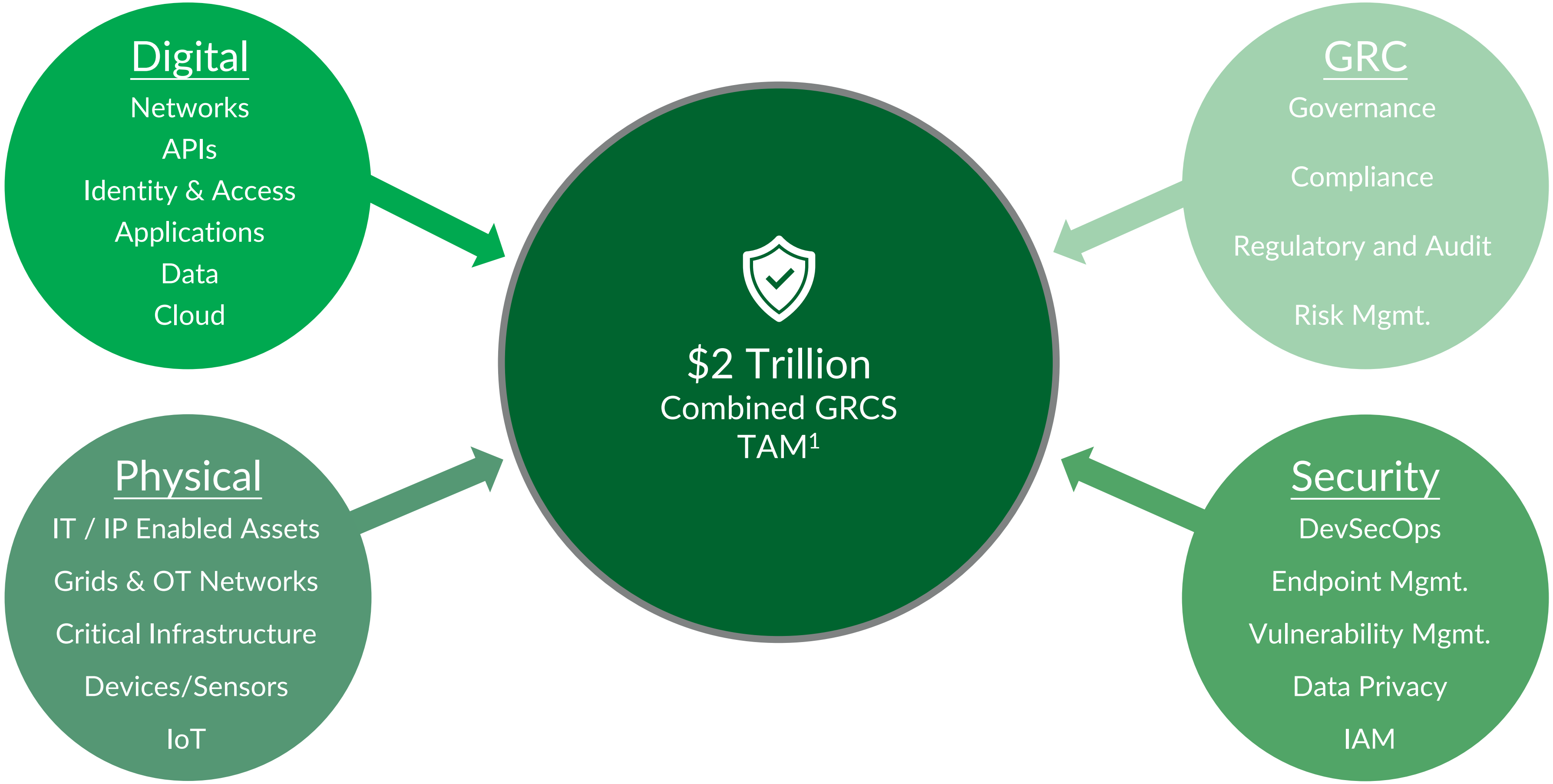
**The "GRCS" market consists of any product / service that helps organizations manage, mitigate and remediate digital risks**

***We see a merging market…***

- The line between what has historically been thought of as "GRC" and "Cyber Security" is increasingly blurring
- Companies building software solving tomorrow's problems can no longer be identified as solely "GRC" or "Cyber Security"

***…Being driven by….***

- Budgets / buyers of the two are relying on the same underlying data sets
- GRC and Cyber Security workflows are increasingly overlapping and mirroring each other
- Changes to the NIST CSF framework imposing new industry standards regarding governance[2]



**Digital**
Networks
APIs
Identity & Access
Applications
Data
Cloud

**GRC**
Governance
Compliance
Regulatory and Audit
Risk Mgmt.

$2 Trillion
Combined GRCS TAM[1]

**Physical**
IT / IP Enabled Assets
Grids & OT Networks
Critical Infrastructure
Devices/Sensors
IoT

**Security**
DevSecOps
Endpoint Mgmt.
Vulnerability Mgmt.
Data Privacy
IAM

CATALYST

*Sources: (1) McKinsey; (2) NIST Cybersecurity Framework*

# Market Dynamics and Tailwinds

| Key Themes | Takeaways and Conclusions | Supporting Evidence |
|---|---|---|
| Digital assets are under attack<br>The attacks are more common and successful | ▪ The advent of digital transformation, catalyzed by remote work, has left organizations more vulnerable than ever to cyber attacks and compliance breaches<br>▪ As organizations access/create more data across more technologies/endpoints than ever before, data compliancy & security becomes more complex and risk exposure remains unprecedented | ▪ Cybercrime **increased 600%** during the COVID-19 pandemic with organizations claiming **threat volumes will continue to double**[1]<br>▪ Corporate data is **doubling** every **12-18 months**[2] |
| Companies must try to prevent attacks, but must also assume defences will fail | ▪ Sophisticated, well-resourced attackers are constantly shifting tactics and building advanced automation tools to exploit new and growing vulnerability gaps<br>▪ We are in the early innings of the *"Security Awakening"* as organizations have accepted that hackers will inevitably breach networks<br>▪ Organizations have shifted from being "reactive" to "proactive" | ▪ **63%** of organizations believe they will be **compromised by a successful attack** on an annual basis[3]<br>▪ **93%** of external attacks **successfully breach an organization's network perimeter** and gain access to company data and resources[4] |
| GRCS products are viewed as necessary insurance by c-suite and boards | ▪ Security breaches are no longer being treated as an "it can happen to anyone" event<br>▪ Companies must be able to show they employed best efforts to protect their digital assets<br>▪ Industry regulators, elected officials and public opinion increasingly do not look kindly upon companies who failed to protect sensitive information | ▪ **83%** of organizations have experienced **more than one** successful data breach[5]<br>▪ Average total cost of a data breach has increased to **$4.4 million** (**increases to $5.6 million** for highly regulated organizations[5]) |

CATALYST

*Sources: (1) McKinsey; (2) Gartner; (3) Herjavec Group; (4) Positive Technologies; (5) IBM*

# Market Dynamics and Tailwinds (Continued)

| Key Themes | Takeaways and Conclusions | Supporting Evidence |
|---|---|---|
| The lack of qualified cyber security professionals is alarming | ▪ Labor shortages of security talent and in-house expertise has forced organizations to turn to 3rd party service providers and automation technologies to fill key knowledge and execution gaps<br>▪ Constantly evolving regulatory complexity and gaps in resources/knowledge will continue to outpace cyber risk management driving need for continued and increased investment | ▪ **1.8 million** shortage of trained security professionals in 2022[1]<br>▪ The market for GRC/Security software and services is expected to reach a **$1.5 - $2.0 trillion TAM** by 2025, 10x estimated size in 2022[2] |
| The government is going to rapidly increase demand for certain security tools and training | ▪ Government is building a more influential position on security standards and allocating resources to bolster protection<br>▪ Increasing path towards US government-enforced standards for private-sector organizations to maintain strong security practices and reward healthy security (already present at public sector level with Biden's Cybersecurity Executive Order issued in May 2021)<br>▪ Enterprises are accelerating investment in security automation tools to get ahead of expanding regulations and to meet new standards | ▪ **40+ US states** introduced **250+ bills** focused on Cybersecurity in 2022 as Cyber legislature becomes increasingly scrutinized[3]<br>▪ EU's GDPR protections impose fines of up to **4% of annual revenue** for customer data breaches |

*Sources: (1) AGC; (2) McKinsey; (3) NCSL*

# GRCS Market Landscape (Rising Stars)

## Training & Awareness

Accredible, CLOUD RANGE
Credly, Curricula
CYBEREADY, CyberVista
CYBRARY, edify
HackNotice, HOOK SECURITY
HOXHUNT, LetsDefend
NINJIO, Opsgility
RANGEFORCE, SIMSPACE

## Governance, Risk & Compliance (GRC)

### Security Compliance & Automation | Security Architecture | Regulatory & Audit | Integrated Risk Mgmt. | Operational Risk Management

6clicks, Apptega, CENSINET, CIRCADIAN RISK, clausematch, CloudSphere, cyberGRX
Panorays, RECIPROCITY, REGOLOGY, CyberSaint SECURITY, CyberSmart, CYBSAFE, DRATA
FASTPATH, SUPPLY WISDOM, TRAVA, trustero, HyperComply, hyperproof, Kion
LAIKA, livingsecurity, LogicManager, Onspring, StandardFusion, whistic, Vanta

## Identity & Access Management (IAM)

### Access Management | Identity Governance & Admin. | Priv. Access Mgmt. (PAM) | Anti-Fraud

bitwarden, britive, Bureau, cerby, ClearSkye
DASHLANE, DEDUCE, evo, jumio, KEEPER, ORY
Quickpass, SECUREAUTH, SECURENDS, SecZetta, SOLOINSIGHT
STRATA, STRIVACITY, zilla SECURITY, SYM, styra

## Security Operations

### Security Analytics (SIEM) | Orchestration (SOAR) | Incident Mgmt. & Response | Vulnerability Mgmt. | Threat Detection & Intelligence

adlumin, ANVILOGIC, Balbix, BISHOPFOX, BLUELAVA, Blumira, CONTRAFORCE, CYBEROWL
Cynamics, CYVATAR, Hunters., Inspectiv, MITIGA, NOPSEC, panther, RAPIDFORT
SNAPATTACK, squadcast, SUREFIRE CYBER From Response to Resilience, SWIMLANE, ThreatConnect, THREATQUOTIENT, tines, vicarius

## Data Protection & Security

### Data Privacy | Data Governance | Ransomware

anjuna, AppOmni, BLACKCLOAK, cyera, CYLERA, DASERA
DATAGRAIL, DNSFilter, ethyca, feroot, neosec, osano, Reblaze
RELYANCE AI, securiti, spec, TRANSCEND, VALTIX, vaultree, veza

## Application Security

### AppSec Testing | Cloud | DevSecOps | API Security

42crunch, APIsec, ArmorCode, Bright, Chainguard
DEVEXUS, grip, perimeter 81, Phylum, QOHASH
ShiftLeft, SYNSABER, THREATX, wallarm, ZORUS

## Infrastructure

### Network | Cloud Infra | Endpoint | IoT

asimily, cervello, CEQUENCE SECURITY, Cyral, KOLIDE
kriptos, Lightspin, netwrix, OKERA
OPSWAT, RACKTOP, Resurface, STACKHAWK

CATALYST

*Note: this landscape is intended to be a representative sampling and is not an exhaustive list.*
*Please direct inquiries to killian@catalyst.com, carson@catalyst.com, grady@catalyst.com*

# GRCS Market Landscape (Leaders and Incumbents)

## Training & Awareness

- HACKTHEBOX
- IMMERSIVELABS
- KnowBe4 Human error. Conquered.
- PLURALSIGHT
- proofpoint
- SECURE CODE WARRIOR
- skillsoft
- QA

## Governance, Risk & Compliance (GRC)

### Security Compliance & Automation | Security Architecture | Regulatory & Audit | Integrated Risk Mgmt. | Operational Risk Management

- ARCHER
- AUDITBOARD
- Avetta
- COALFIRE
- Diligent
- FUSION RISK MANAGEMENT
- ORIGAMI RISK
- metricstream
- OneTrust
- LOGICGATE
- ProcessUnity
- riskonnect
- intertek SAI GLOBAL
- SecurityScorecard

## Identity & Access Management (IAM)

### Access Management | Identity Governance & Admin. | Priv. Access Mgmt. (PAM) | Anti-Fraud

- 1Password
- arcon
- BeyondTrust
- CYBERARK
- Delinea
- ForgeRock
- jumpcloud.
- okta
- ONE IDENTITY
- PingIdentity
- SailPoint
- SAVIYNT
- WALLIX

## Security Operations

### Security Analytics (SIEM) | Orchestration (SOAR) | Incident Mgmt. & Response | Vulnerability Mgmt. | Threat Detection & Intelligence

- splunk>
- securonix
- sumo logic
- tenable
- DARKTRACE
- RAPID7
- Qualys.
- red canary
- LogRhythm
- KENNA Security
- HUNTRESS
- Secureworks
- servicenow

## Data Protection & Security

### Data Privacy | Data Governance | Ransomware

- BigID Know Your Data
- CODE42
- druva
- hp
- imperva
- NetApp
- PKWARE
- PROTEGRITY
- TrustArc
- VARONIS

## Application Security

### AppSec Testing | Cloud | DevSecOps | API Security

- aqua
- Checkmarx
- Contrast Security
- MEND
- noname
- SALT SECURITY
- snyk
- sysdig
- VERACODE
- TRACEABLE

## Infrastructure

### Network | Cloud Infra | Endpoint | IoT

- cisco
- CLOUDFLARE
- CROWDSTRIKE
- ivanti
- JUNIPER NETWORKS
- FORTINET
- LACEWORK
- Malwarebytes
- McAfee
- mimecast
- orca security
- paloalto NETWORKS
- SentinelOne
- SOPHOS
- THREATLOCKER
- tufin
- vmware
- WIZ

CATALYST

*Note: this landscape is intended to be a representative sampling and is not an exhaustive list.*
*Please direct inquiries to killian@catalyst.com, carson@catalyst.com, grady@catalyst.com*

# GRCS Market Landscape (Categories Defined)

## Training & Awareness

*Helps employees learn how to either 1) use cybersecurity products, 2) avoid becoming a victim of a cyber attack*

## Governance, Risk & Compliance (GRC)

Security Compliance & Automation | Security Architecture | Regulatory & Audit | Integrated Risk Mgmt. | Operational Risk Management

*Helps organizations identify, manage and mitigate business risks, as well as stay in compliance with relevant laws, regulations and standards that apply to their business activities*

## Identity & Access Management (IAM)

Access Management | Identity Governance & Admin. | Priv. Access Mgmt. (PAM) | Anti-Fraud

*Helps organizations keep track of who is allowed to use different systems/resources and provision access to ensure that only the right people can access the right things with the goal of maintaining data security and privacy*

## Security Operations

Security Analytics (SIEM) | Orchestration (SOAR) | Incident Mgmt. & Response | Vulnerability Mgmt. | Threat Detection & Intelligence

*Helps security teams monitor, identify, assess, analyze and respond to security threats, vulnerabilities or breaches*

## Data Protection & Security

Data Privacy | Data Governance | Ransomware

*Employ monitoring, filtering, blocking and remediating technologies to address the risks of inadvertent or accidental data loss and the exposure of sensitive data*

## Application Security

AppSec Testing | Cloud | DevSecOps | API Security

*Address and remediate security vulnerabilities in the process of the designing, coding, configuring and deploying software applications*

## Infrastructure

Network | Cloud Infra | Endpoint | IoT

*Protect IT network infrastructure and devices from digital attacks*

*Please send any inquiries to killian@catalyst.com, carson@catalyst.com, grady@catalyst.com*