AGILE GRC

The mindset, techniques and tools employed by an emerging breed of Agile GRC practitioners in organizations running SAP.

Pubished 2020

soterion

soterion.com

> “Faster, better, more” has become the baseline of expectations in the digital world. Now is the time for governance, risk management and compliance (GRC) functions to participate in shaping the future in the digital world.

Content

01

Why Agile GRC?

> Change is the single greatest governance, risk and compliance (GRC) business challenge today...
>
> - Michael Rasmussen, a highly regarded GRC thinker

He continues, **"organizations often fail to monitor and manage access controls efficiently and effectively in an environment that demands agility."**

It's a reality that GRC practitioners are facing a continuous barrage of SAP access complexity, as well as regulatory and business change. Rasmussen says **"Often, existing SAP access risk tools are dated, cumbersome, too costly to own and maintain, and lack the ease-of-use and intuitiveness that the business needs to understand SAP access risk and related processes."**

The point is clear: A more agile approach is required in the face of accelerating change, it cannot be "business as usual" for GRC practitioners.

But what does 'agile' actually mean?

02

What does it mean to be an agile organization?

The agile approach originated in the software development industry, and essentially emphasized collaborative product delivery over everything else.

It took formal shape in the publication of the Agile Manifesto in 2001, and almost immediately caught on with organizations in industries beyond software development as offering a better way to work, given today's fast pace of change.

Agile's four guiding principles are:

Individuals and interactions over processes and tools

Working software (i.e. products or services) over comprehensive documentation

Customer collaboration over contract negotiation

Responding to change over following a plan

I'm sure you'll agree that these four principles have a ring of truth about them, irrespective of your field or industry.
They seem to offer timely wisdom in today's fluid world of work.

03

As the ideas enshrined in the agile approach gained ground, it began to dawn on organizational thinkers that the agile approach represented more than a new project management methodology; more fundamentally it represented an alternate organizational paradigm – that is, a new lens of what an organization is. Let me explain.

Frederick Taylor pioneered the idea of scientific management in the 1900's, which was successfully adopted by companies like Ford. The approach essentially viewed an organization as a machine, and leveraged hierarchies, specialization and scientific process optimization to produce unprecedented results. This "organization as machine" paradigm was the prevailing view of organizations until early this century.

Trends have emerged over the last 20 years which have disrupted the old paradigm – environments around organizations changing at an unprecedented rate, a constant stream of disruptive technologies compelling organizations to adapt or die, and the internet's democratization of information have all had far-reaching implications for organizations. This gave rise to the agile approach and extended its application beyond just its way of collaborating to the organization's entire way of being.

Mckinsey consolidated their view of an agile organization in 2018 to include the following characteristics:

STRUCTURE
Network of empowered teams

- Clear, accountable roles
- Hands-on governance

PROCESS
Rapid decision iteration and continuous learning

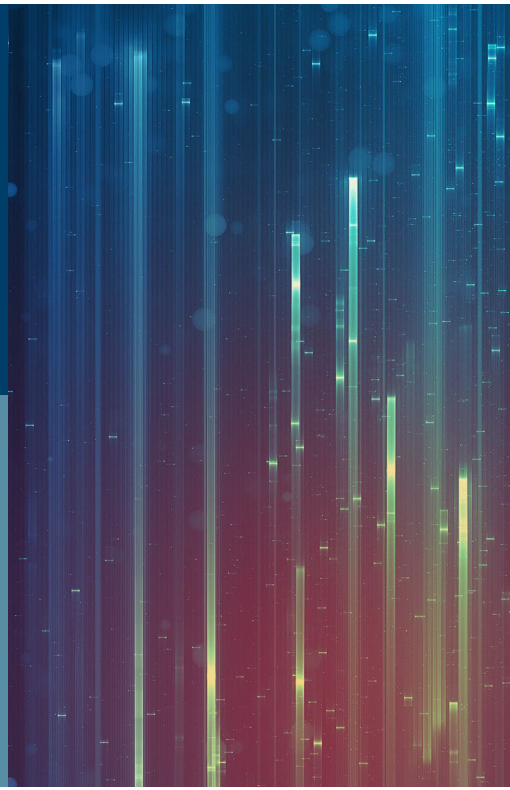
- Rapid iteration and experimentation
- Hands-on governance

PEOPLE
Dynamic people model, role mobility, fluid workforce

- Cohesive community
- Entrepreneurial drive
- Role mobility

TECHNOLOGY
Next generation enabling technology

- Evolving technology architecture
- Next-generation technology development and delivery



04

What does this mean for GRC?

Things are moving faster all around us. Agile thinking encompasses the idea of "clock speed" i.e. the pace at which an organization, as an entire system, is able to move, react, adapt and so forth.

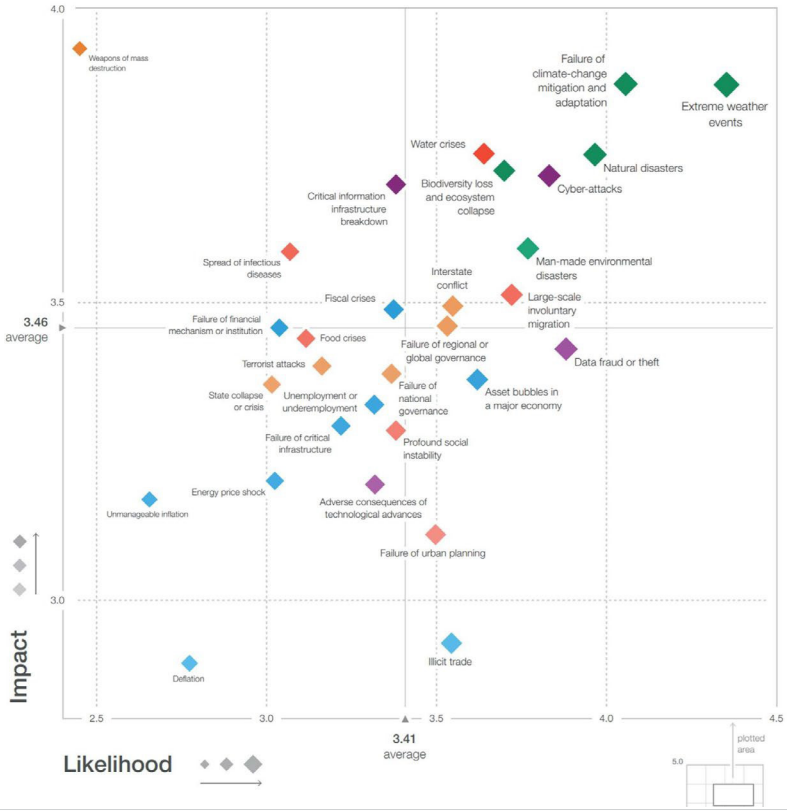
It's estimated that today's average large organization requires a clock speed 3-5 times faster than the equivalent organization a decade ago.

Whilst agile thinking has brought great benefits to organizations in increasing their clock speed, it has also brought with it a significant misconception about GRC. In the pursuit of agile delivery, GRC can easily be seen as part of the 'old paradigm' and hence ignored or undervalued. Alternatively, even if the GRC function is appreciated by business, GRC practitioners often fail to adapt their approach to the new clock speed realities. The effect of both scenarios is highlighted in the recent 2019 WEF Report on significant global threats. The report lists both cyberattacks and data fraud as likely, high impact global threats in the near future. This underscores the fact that GRC in terms of impact, is more critical and the stakes are higher than ever before should we fail to get it right.

GRC principles fit well with the agile approach, and are more relevant and important than ever before. Getting GRC right in an agile environment depends on having the right mindset, approach and tools. We'll look at each of these in turn.

The Global Risks Landscape 2019

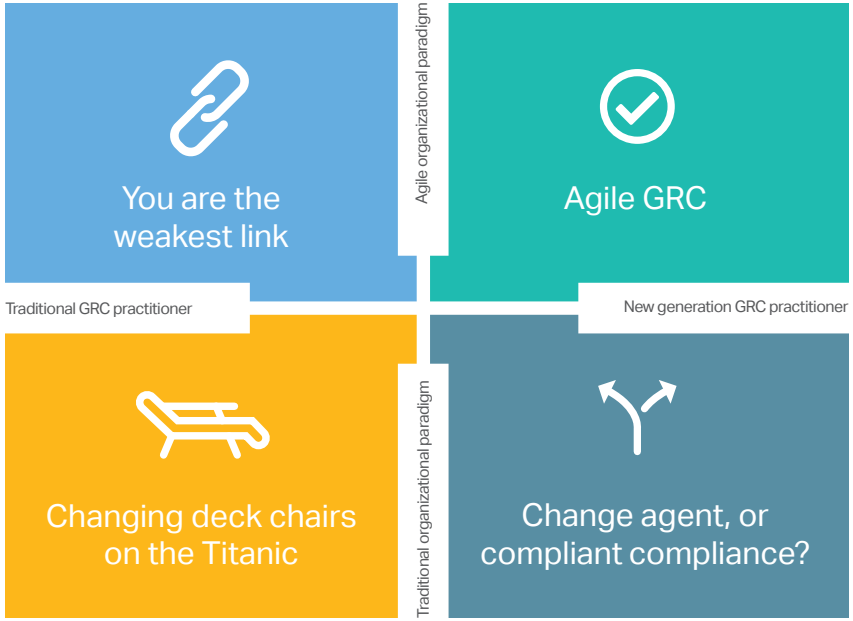
Increase in Cyberattacks and Data Fraud or Theft



05

The right mindset

We said earlier that GRC principles fit well with an agile approach. But, and this is an important *but:* making GRC work doesn't only depend on the organization making the leap to agile; it also depends upon GRC practitioners making the personal leap from an old to a new paradigm. Consider the following four scenarios:



McKinsey 2018
www.mckinsey.com/business-functions/organization/our-insights/the-five-trademarks-of-agile-organizations

You are the weakest link

The organization has evolved to embrace an agile approach, but the GRC practitioner is stuck in the previous paradigm. Here the GRC practitioner views organizational changes as irresponsible trends and tries to champion a return to more 'credible' practices, perhaps even become a legalistic enforcer of (outdated) compliance protocols. Sadly, the GRC practitioner is missing the point and is hindering effective new generation GRC in their organization.

Changing deck chairs on the Titanic

On the ill-fated Titanic, a well-meaning deck hand may have decided it was sensible to re-arrange deck chairs to make things ship-shape, sadly unaware of the ultimate irrelevance of his actions. Similarly, where the GRC practitioner and organization both adhere to the 'organization as machine' paradigm, the system isn't equipped to adapt to changes in the world around it and hence its sustainability is of major concern. Against that backdrop, iterations to its GRC practice may be internally sensible, but akin to re-arranging deck chairs on the Titanic given the external threats.

Agile GRC

The organization has become more responsive to its environment, able to adapt products and services more quickly than competitors. Its GRC practitioners see this agility as a positive culture and implement agile processes and tools to enable effective GRC.

Change agent or compliant compliance?

Many GRC practitioners find themselves in this quadrant. They are new generation GRC practitioners operating in a traditional organization. They face a decision - either be an advocate for change or simply go through the motions and deliver the kind of GRC the organization requires. Could someone in GRC influence organization-wide change? We believe the answer is, yes! With a 'courageously pragmatic' approach one could advocate for company-wide change (possibly finding kindred spirits within your organization), whilst at the same time pragmatically delivering GRC requirements within the prevailing framework.

07

The right approach

So, what is the right approach for agile GRC? Given that organizations differ vastly by industry, regulatory environment, GRC maturity and so forth, there is no 'one-size-fits-all' answer to this, but we'll outline a couple of agile GRC descriptors, and then provide a practical framework for organizing your GRC in an agile way.

User-Centric

Adaptive

Rapid

Connected

Continuous Delivery

Trusted

08

Agile GRC is user-centric

Agile GRC realizes the need for engaged business users, and hence puts business users at the centre of the process. GRC language is converted into a language business users can understand. Enhanced ownership is further achieved through more intuitive tools, for example introducing business process visualizations that help business users contextualize and understand risks.

Putting the business users at the centre of the process

Enhancing accountability & ownership through visualization and collaboration

Converting GRC language into a language the business users can understand

Lack of engaged business users has always been the Achilles heel of GRC. Research shows it is the leading cause of GRC implementation projects floundering. Engaged business users are more vital than ever given the fluidity of organizational environments today. GRC must become a team sport!

FIRST LINE	SECOND LINE	THIRD LINE
Operational users	Risk and compliance department	Audit and assurance

Consider the audit principle of "Three Lines of Defence". If business users, the first line of defence, are unengaged, it falls to the GRC team to ensure that access risk remains healthy. This is usually done in an episodic fashion, frequently timed to coincide with an audit. The power of engaged business users is manifold: there are many of them, and they know and understand their processes better than anyone. Giving them the means to monitor and respond to the risks inherent in their processes, provides a powerful first line of defence which in turn allows for the GRC team to play a more strategic, value-adding role.

Agile GRC is adaptive

Traditional GRC tools are built upon static rule sets, which should be reviewed 'from time to time' to adapt them to any changes in business process flows. The traditional paradigm assumed such process flows seldom change. In reality, with today's pace of change and agile ways of working, access risk simulations are performed against rule sets that are increasingly out of touch with an organization's reality. Business users become frustrated by this and their buy-in diminishes accordingly.

New generation GRC tools recognize that business process flows are dynamic and fluid, and hence build dynamic rule sets with adaptive capabilities. Machine learning technologies often play a role here. Another approach is 'crowdsourcing' rule set changes from business users themselves, through intuitive visualizations that keep GRC tools relevant and hence keep business users engaged.

Agile GRC is rapid

Traditional applications typically have a software license to implementation cost ratio of between 1:3 and 1:5. That is, for every dollar in licensing in the first year, the organization can expect to pay up to 5 dollars in configuration. The implementation process itself is often the organizational equivalent of open-heart surgery, given the sheer intensity of the process.

New generation GRC applications are typically implemented at least 50% faster than traditional applications. This translates into lower total cost of ownership, less business disruption and quicker establishment of GRC capability.

Aside from the cost-saving implications of rapid deployment, Agile GRC configurations allow users to "fail faster" in the positive sense of getting vital feedback on access simulations and adverse process changes quicker, which allows for timeous adjustments.

Agile GRC is connected

Agile GRC vendors are connecting their applications with other vendors from similar but different fields in order to provide a more holistic offering. Examples of this are integrations with Identity Access Management solutions, Enterprise Risk solutions, Process Control solutions and Business Process Mining solutions.

The API economy enables organizations to choose the exact applications they require given their current business landscape, and to create a "one size- fits-one" GRC technology ecosystem that fits their needs. This contrasts with the traditional "one-size fits-all" idea of one monolithic GRC application which caters for every conceivable scenario.

Agile GRC offers continuous delivery

As SAP move more functionality to the cloud (SuccessFactors, Ariba, Concur etc), as well as customers starting to replace non-core SAP products with 3rd party solutions such as Salesforce.com and WorkDay, GRC solutions need to be able to analyze non-ABAP based solutions. Agile GRC solutions are future proof, in that they will be able to seamlessly analyze access risk from traditional SAP systems (ABAP), as well as SAP cloud solutions and 3rd party solutions.

Agile GRC is trusted

Managing access risks is both time consuming and laborious. Using historical data to develop trust relationships will allow GRC practitioners and business users to focus on the exceptions. Examples of this include monitoring transaction usage activity and highlighting exception transaction codes. Or, knowing which terminal the user accesses SAP from, and highlight any activity from a different (non-trusted) terminal.

The right framework

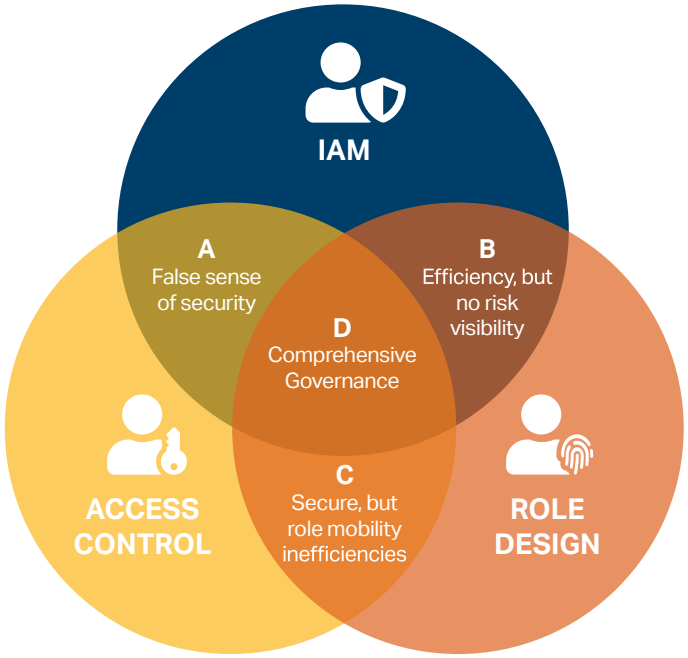
Hopefully we have been able to explain the value of agile GRC to support your agile organization. Now let's go a little further and look at SAP security more practically, considering a framework including the following security components:

SAP Role Design

Governance, Risk & Compliance - Access Control

Identity Access Management

Although there are more security components available, the importance and inter-relationship between these three components form the backbone of effective Agile GRC within an SAP environment.



Consider the three overlapping circles

A. False sense of security

For those organizations who implement access control and identity management solutions, but do not place much importance on the underlying role design. If the organization's roles are outdated and providing SAP users with inappropriate access, the value of the access control and IAM solutions are diminished due to the underlying role design.

B. Efficiency, but no risk visibility

For those organizations who have addressed their underlying role design and implemented an identity management or governance solution. These organizations will have efficiencies around leaver/joiner/mover and access provisioning, but they do not have visibility of their risks. Many of these organizations may have access control solutions, but it is not integrated into their IAM solution.

C. Secure, but role mobility inefficiencies

For those organizations who have addressed their underlying role design and implemented an access risk solution. These organizations have secure SAP solutions, but they lack efficiencies around leaver/joiner/mover and access provisioning.

D. Comprehensive, agile GRC

Where the organization has addressed their underlying role design, implemented an agile access risk solution as well as an identity access governance solution. This is where the organization will benefit from comprehensive SAP Governance.

The right tools

As noted earlier, the rise of API-led connectivity has opened an array of GRC application options to organizations which were previously not feasible. This makes it impossible for us to make a blanket recommendation of tools A, B or C for your specific context. The main message to convey is that today's GRC practitioners in an SAP environment enjoy choice, and are able to architect their own, fit-for-purpose GRC ecosystem.

Courageous, new generation GRC practitioners are making GRC tool decisions based on new ways of creating value for increasingly agile organizations, rather than opting for the supposedly 'safer,' more traditional route.

Here are some considerations to keep in mind in selecting appropriate tools:

Is this tool really business-user friendly?

- Will business users see value in the tool?
- Is the tool intuitively designed in terms of interfaces and navigation?
- Is the learning curve steep or is the tool easy to become conversant with?
- Does the tool provide visualizations of business processes that are recognizable to business users?
- Does the tool have a good track record of business-user adoption in existing implementations?

Is this tool built to adapt to a fast-moving, fluid environment?

- Does the tool have a 'set-and-forget' static approach to risk rulesets?

S/4HANA and SAP Cloud

- Is the tool S/4HANA ready, able to assess Fiori access?
- Is the tool capable to performing risk analysis on SAP Cloud products like SuccessFactors and Ariba?
- If the tool is ABAP based, will it be future-proof i.e. will it be able to connect to 3rd party applications like Salesforce and WorkDay.

Is the tool 'size-sensible' for the size and complexity of our organization?

- Does the tool offer all functionality essential to our organization?
- Does the tool offer functionality superfluous to our requirements, which would negatively impact user adoption and cost?

Is this tool rapid to implement and achieve ROI on?

- What is this tool's envisaged implementation duration?
- What is this tool's envisaged implementation cost?
- Are there examples of comparable organization's implementation journeys I can learn from?

Important considerations in GRC tool selection

In our increasingly fast-paced world, there is a strong correlation between successful GRC and levels of business user engagement in SAP organizations. Therefore, evaluation of tools in terms of attributes which contribute to business user engagement is an appropriate evaluation lens to employ.

Conclusion

We're living through an era hallmarked by a rapid increase in the rate of change in the marketplace. Organizations are being forced to adapt to the new realities. Successful organizations are becoming more agile in their ways of working.

Whilst traditional GRC practitioners may view these recent developments in a negative light, new generation GRC practitioners are seeing the opportunity for GRC to play a greater role in proactive value creation than ever before, and are embracing new agile technologies and methodologies in doing so.

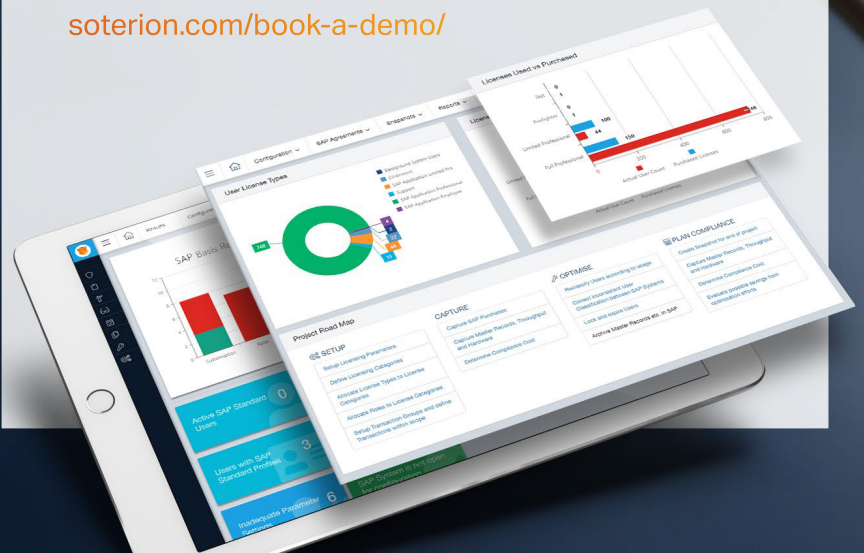
Soterion. Powerful features, a pleasure to use.

Soterion has reimagined GRC from the ground up to offer an unparalleled GRC solution to organizations running SAP. It's popular features combine with an award-winning user experience, delivering a solution that's quick to install, easy to learn and S/4HANA ready.

Experience a better way of managing GRC, today.

Book a Demo

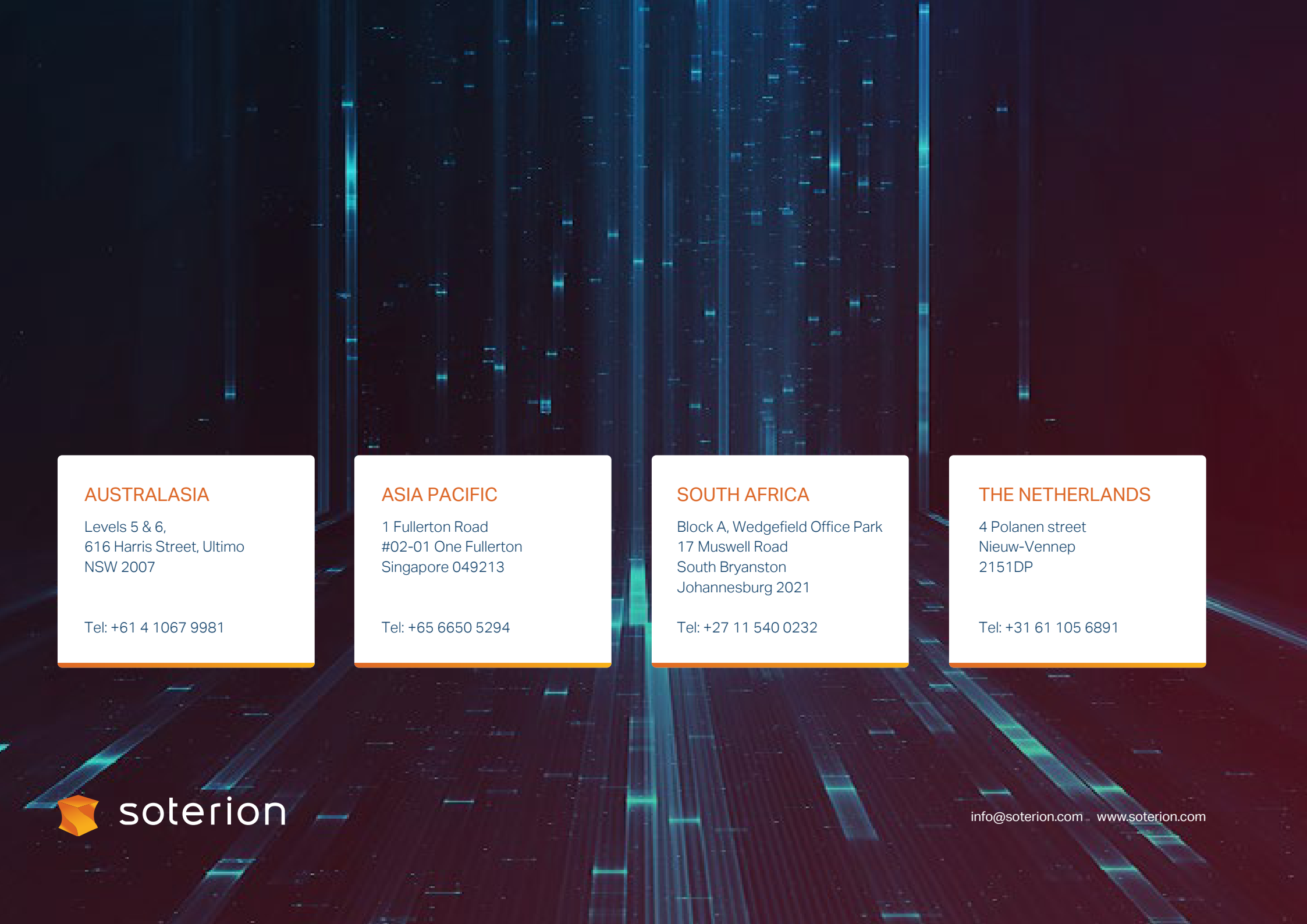
soterion.com/book-a-demo/



User Experience Winner

EXPERIENCE 2019

grc2020



AUSTRALASIA

Levels 5 & 6,
616 Harris Street, Ultimo
NSW 2007

Tel: +61 4 1067 9981

ASIA PACIFIC

1 Fullerton Road
#02-01 One Fullerton
Singapore 049213

Tel: +65 6650 5294

SOUTH AFRICA

Block A, Wedgefield Office Park
17 Muswell Road
South Bryanston
Johannesburg 2021

Tel: +27 11 540 0232

THE NETHERLANDS

4 Polanen street
Nieuw-Vennep
2151DP

Tel: +31 61 105 6891

soterion

info@soterion.com www.soterion.com