

Is Your 3rd-Party Risk Program Ready for the Next Supply Chain Crisis?

Brenda Ferraro

Vice President, Third-Party Risk
Prevalent

Steve Roesing

CEO
ASMGi



Your Presenters



Brenda Ferraro
VP, Third-Party Risk
Prevalent



Steve Roesing
President, CEO
ASMGi

Agenda

Accelerating procurement and sourcing

Expanding sources of vendor risk intelligence

Working with suppliers to proactively reduce risk and ensure compliance

Driving more informed, risk-based decision making across your organization

What are the challenges with accelerating procurement and sourcing?

Procurement & Sourcing

Supply Chain Universe

Visibility on all vendors IT, OT, Manufacturing, Transportation, etc.

Govern and manage the supply chain lifecycle from onboarding to termination

Develop a preferred supply chain list of vendors with mature security and resiliency

RFx & Selection

Provide rapid information using threat intelligence

Use the scoring and thresholds to provide risk scoring as part of the overall segmentation

Receive information on maturity acumen prior to selection

Profiling & Context

Capture context on supply chain and outsourcing chain engagements for proper due diligence

Create tags and identifiers for reporting to account for relationship mapping

Sets up tiering and prioritization

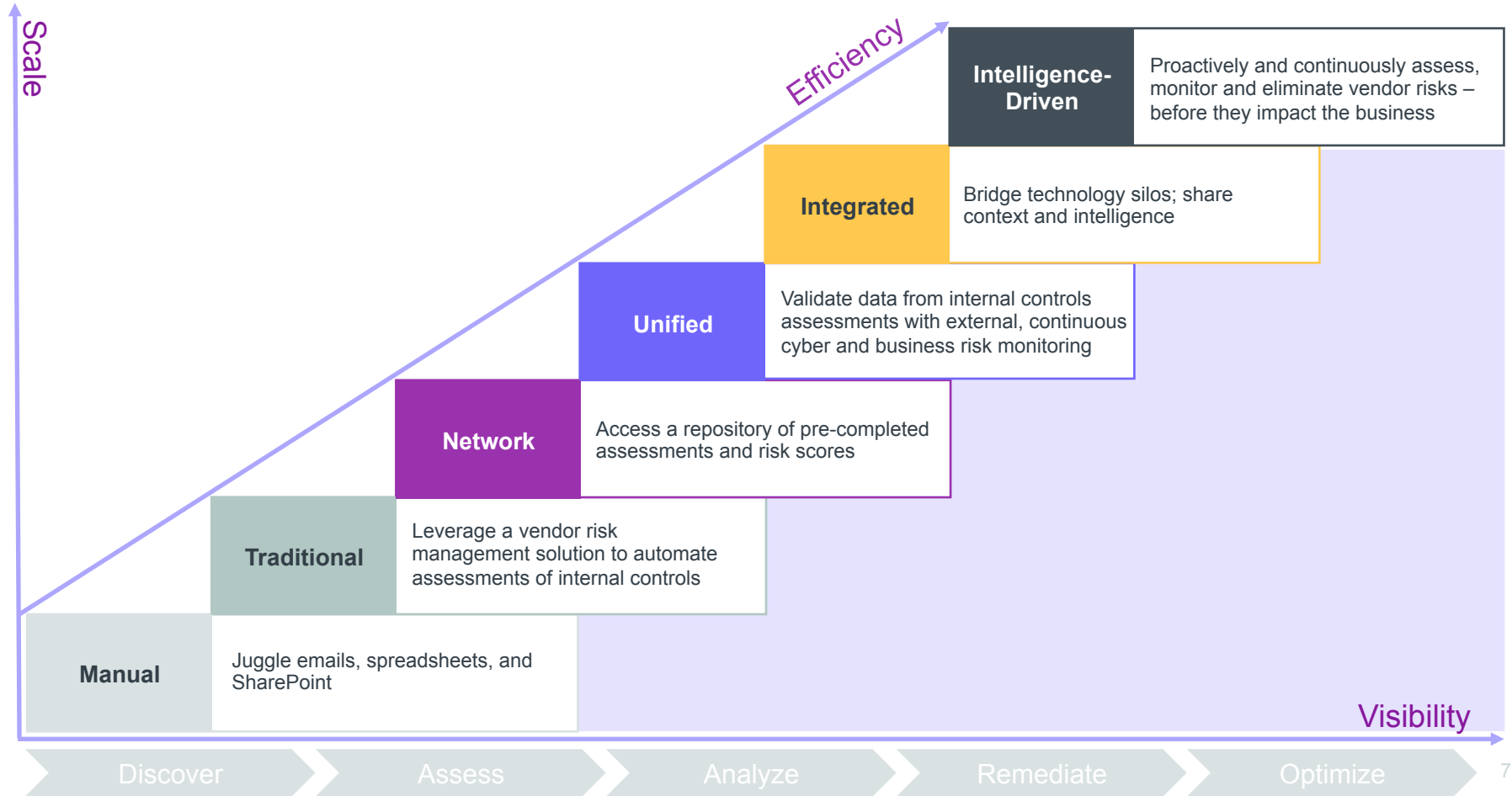
Inside Out & Outside In

Gather and normalize responses via questionnaires and threat intelligence to identify true risk

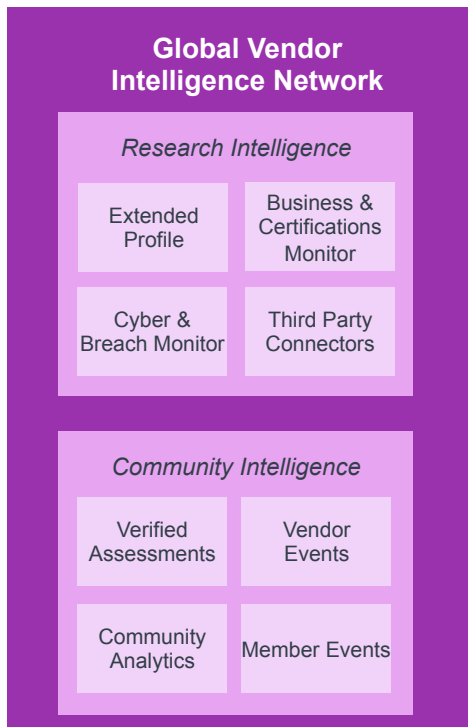
Provide ongoing and continuous evaluation intelligence as risks are identified, monitored and mitigated

Are you seeing an expansion in the sources of vendor risk intelligence?

Efficiency, Visibility and Scale



Add Speed and Scalability with the Vendor Intelligence Network



Assessment Libraries Add
Speed and Scale

Vendor Community

- Proactive assessments
- Certifications
- Docs & agreements
- Events

Vendor Risk Intelligence

Continuous, comprehensive, relevant:

- Global research
- Assessments
- Partner feeds

Private Sources

- Credit reports
- Risk scores
- Financials
- Payments
- Legal Actions
- Certifications
- 65+ threat feeds
- 50+ paste sites
- Blogs & social media
- Code repositories
- 1.5k+ hacker forums
- Dark web (80+ forums)

Completed Assessments

- 10,000+ verified records
- Sig-Lite/Sig-Core
- Prevalent Compliance Framework (PCF)
- Cybersecurity Maturity Model Compliance (CMMC)

Regulatory Monitoring

Coverage across 15+ regulations and frameworks:

- CAIQ
- CMMC
- GDPR
- HIPAA
- ISO
- NIST
- NYDFS
- PCI
- And more

Public Sources

Business & breach monitoring across 200k+ sources

- Data breach sites
- Corporate sites
- News feeds
- Trade publications
- Industry sites
- And more

Technology Integrations

- ServiceNow
- RSA Archer
- BitSight
- And more

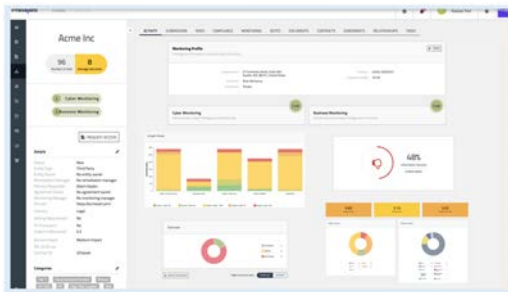
Industry Partnerships

- H-ISAC
- LVN
- Legal Theorem
- Shared Assessments

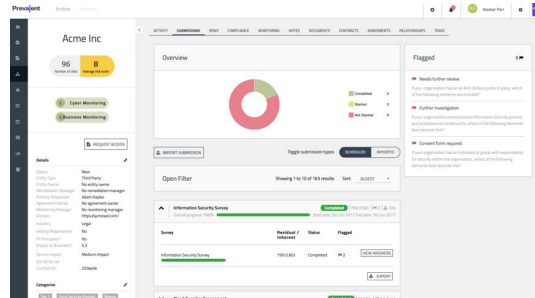
What techniques work well to proactively reduce risk and ensure compliance?

Scaling With Quality

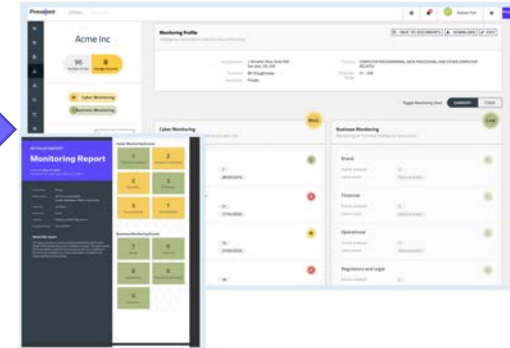
Entity Profiling/Onboarding



Assessment Insights



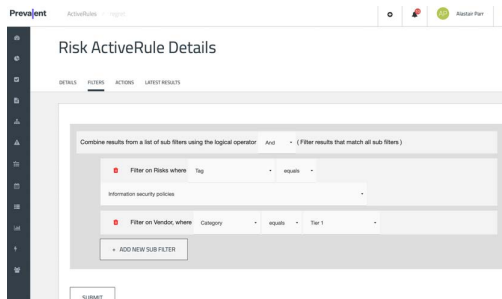
Continuous Monitoring Insights



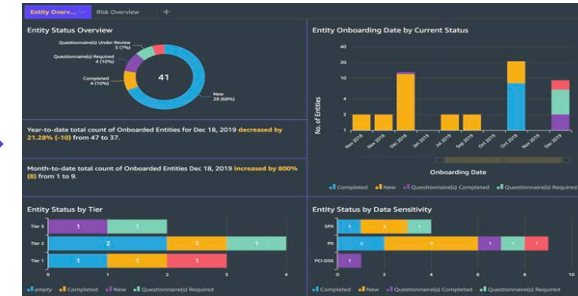
Normalized Risk Insights



Playbook Automation

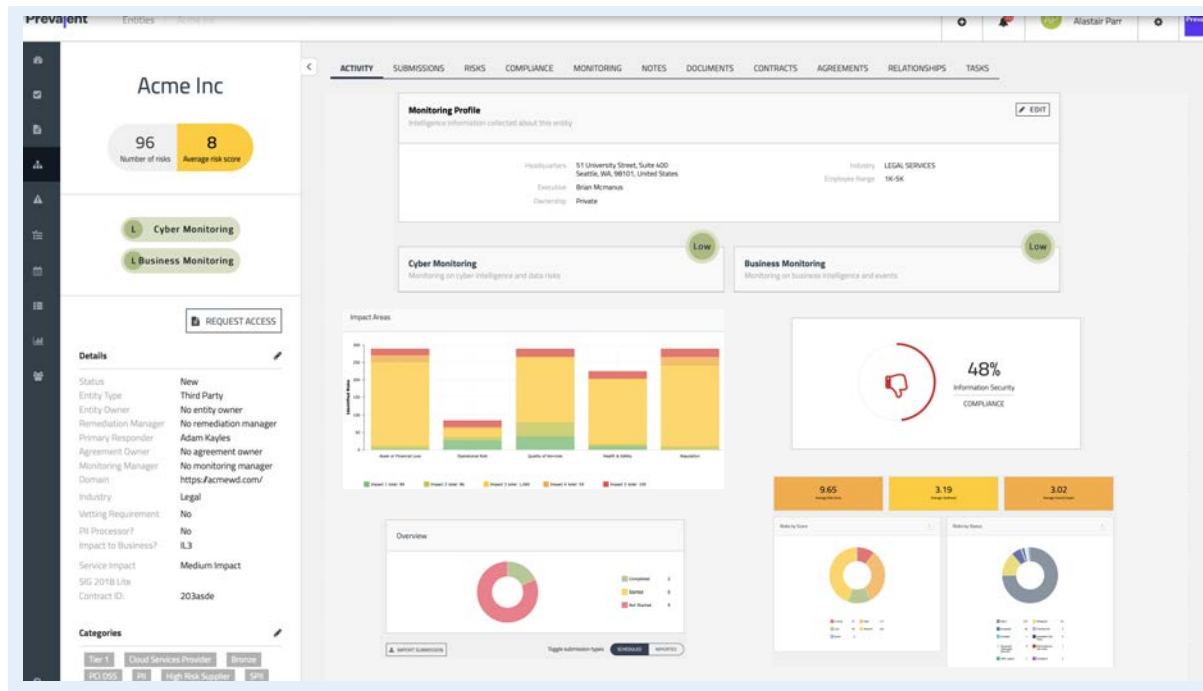


Aggregated Reporting Insights



Entity Profiling

Review a **Comprehensive Profile of Risk, Compliance, and Context** on a single page for vendors or internal business functions. Profile Data is importing from the Intelligence Network and/or connected system integrations.



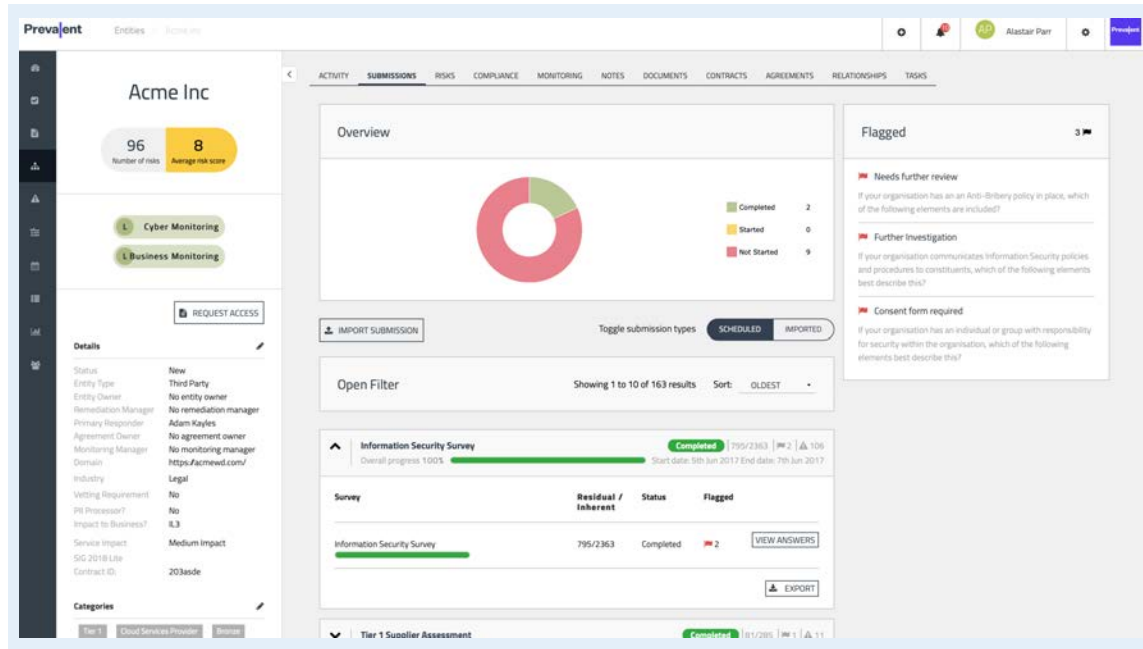
Risks captured from assessments and automatically translated from monitoring feeds.

Compliance correlated from predefined or custom mappings against domains.

Context regarding what they do and how collated from business feeds and verified by entity owners.

Assessment Insights

Assessments drive **automatic risk identification** and give insight into policy and process. **Proactive Assessments** allow for regular and opportunistic information gathering, including event management. Assessment Insights can be importing from the Intelligence Network and/or from launching vendor assessments using automation playbooks.



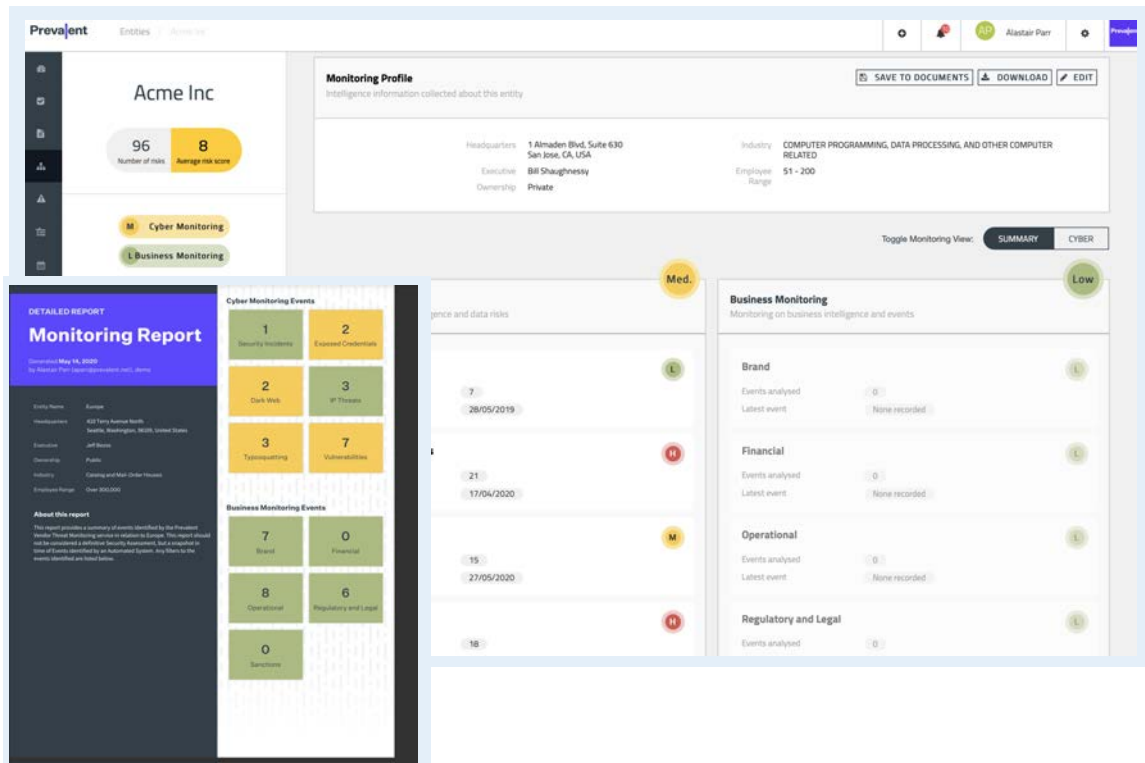
Scheduler allows regular assessments and chasers to entities from a broad range of library assessments

Auto Inherent/Residual Risk identified automatically from every assessment, factoring ongoing management.

Self-Reporting ability for entities to report an event which requires action.

Continuous Monitoring Insights

Continuous Monitoring includes **Cyber, Business, and Financial Events synchronized daily**. External feed data can provide **actionable intelligence**. Monitoring Insights can be importing from the Intelligence Network and/or from enabling continuous monitoring using automation playbooks.



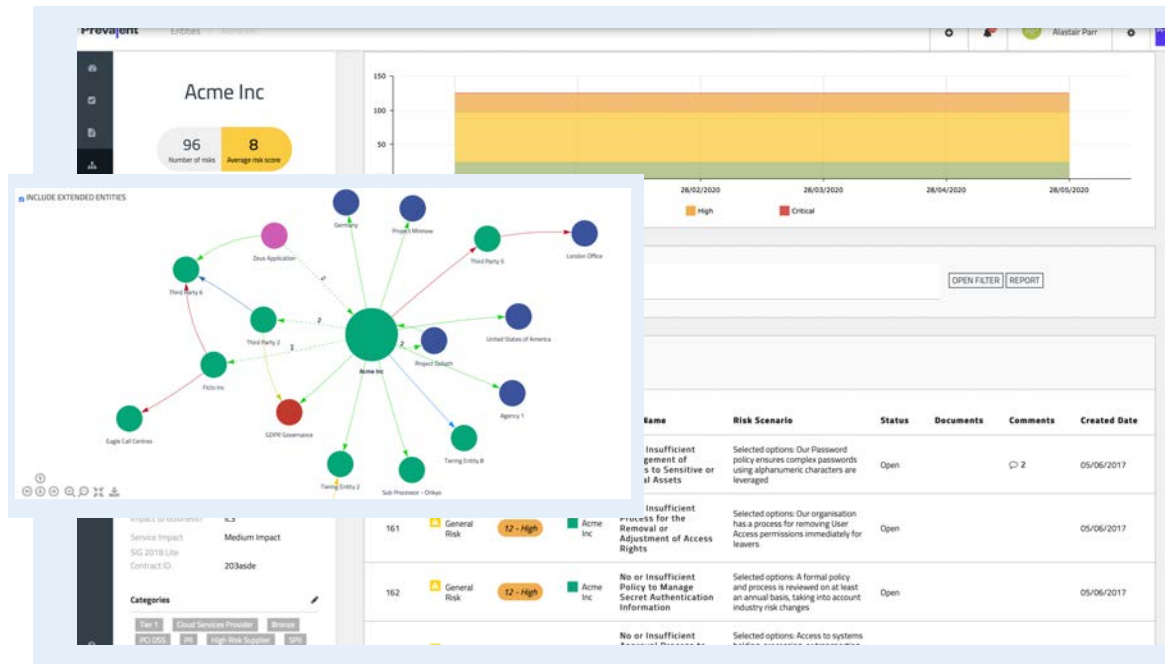
Actionable through automatic risk creation, tasks, and review flags.


Reportable through either the Platform risk reporting, or via generated PDF reports with executive summaries.


Contextual Mappings through risk relationships which correlate results to assessment, audit, or compliance findings.


Normalized Risk Insights

All Data is Normalized as Risks, providing a mechanism for consistent remediation, reporting, and analytics. This feeds into a AI/ML analysis engine for powerful insight. Risks are quantified and infused with additional context and relationship mapping.



 **Automatic Creation** of risks from continuous monitoring, profiling, and assessments.


 **Guided Remediation** via proposed actions, task allocation, and automated status changes.


 **Contextual Associations** through risk relationships, providing context and compensating controls.


Program Playbook Automation

Automation Libraries provide custom or default templates that can be linked into playbooks to enable automation of program functions such as onboarding, assessment distribution, monitoring enablement, risk triage, risk remediation, and approvals.

The screenshot displays the 'Risk ActiveRule Details' interface in the Prevalent application. The top navigation bar includes the Prevalent logo, 'ActiveRules', and a breadcrumb trail ' / > / regret'. On the right, there are icons for settings, notifications, and a user profile for 'Alastair Parr'. The main content area has tabs for 'DETAILS', 'FILTERS', 'ACTIONS', and 'LATEST RESULTS', with 'FILTERS' currently selected. Below the tabs, a section titled 'Combine results from a list of sub filters using the logical operator And' shows a configuration for filtering risks. It includes two sub-filters: 'Filter on Risks where Tag equals Information security policies' and 'Filter on Vendor, where Category equals Tier 1'. A '+ ADD NEW SUB FILTER' button is located below these filters. At the bottom left, there is a 'SUBMIT' button.

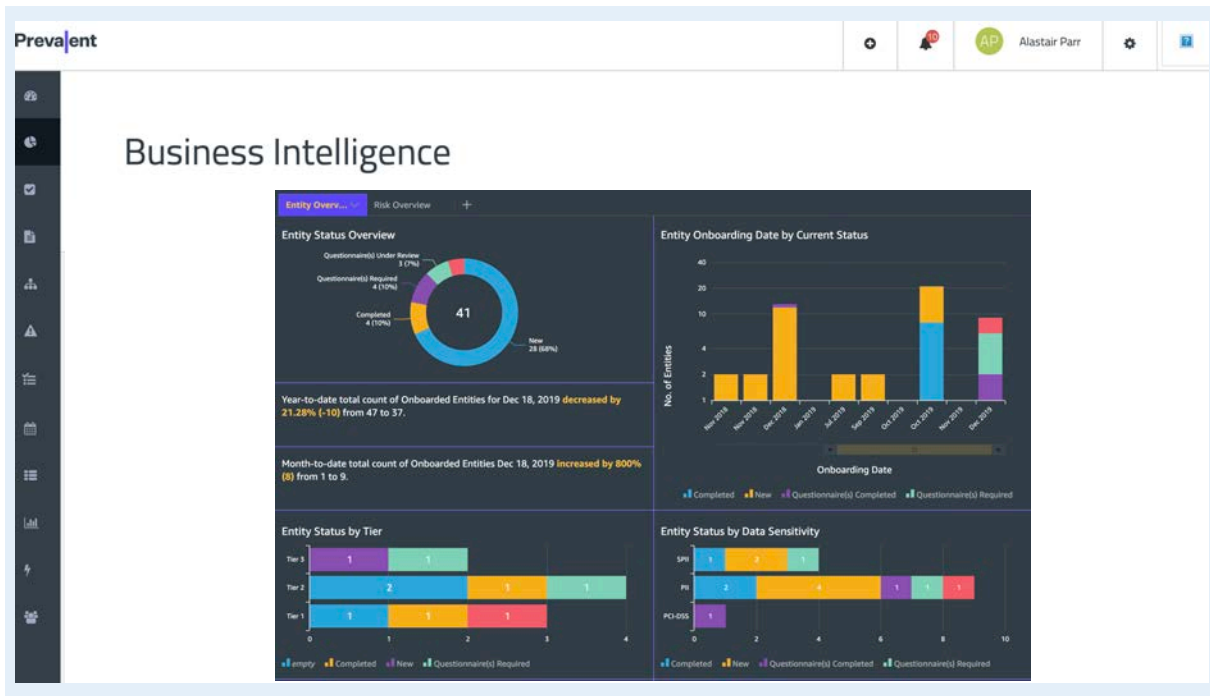
 **Granular Triggers** mean automatic workflows can be created for any customer use case.

 **Risk Modification** can be automated based on the entity, for example Tier 1s are prioritized, or monitoring results correlated against assessment results.

 **Human Triggers** allow users to validate the automated workflow for audit trails.

Aggregated Reporting Insights

Machine Learning/ AI Reporting through customized dashboard and notifications. Reporting and Analytics on workflow progress, assessments, monitoring, risks, and user behavior.



Customized Dashboards

leverage a library of templates built for different program role requirements.



Exception Identification

integrated machine learning automatically highlights any results or user behavior which does not conform to normal activity.



Automated Insights

show any identified trends or examples of entities which require additional focus.







































Are there unconventional ways to drive more informed, risk-based decisions across an organization?

How to Visualize the Full Risk Picture



Focuses on driving a common workflow, providing **automation** to accelerate the program while delivering **actionable insights**. This is provided through **comprehensive profiles** of entities.

Powerful Capabilities at Every Stage of TPRM Maturity

Stop the Pain		Make Intelligent, Informed Decisions		Adapt & Grow
Traditional Assessment	Network Global Vendor Intelligence Network	Unified Assessment + Monitoring	Integrated APIs & Connectors	Intelligence-Driven Analytics & Automation Engine
 Standardized Questionnaires	 Pre-completed and verified assessments	 Cyber monitoring: public sites; deep/dark web	 Reduce onboarding time by up to 85%	 Multi-dimensional analysis
 50+ Standard Assessments	 80%+ reduced onboarding time (15 days avg.)	 Business monitoring: financial, legal, brand, etc.	 RESTful API w/ 65+ endpoints & attributes	 Behavioral analytics & detection
 Custom Assessments	 Continuous cyber monitoring, scoring & alerting	 Risk-based decision-making	 Sync vendor profiles and risk ratings	 Uncover hidden risks
 Proactive & incremental assessments	 Deep vendor inspection for profiling, tiering & monitoring	 Single view of top risks	 Connectors for ServiceNow, Archer & Ariba	 Action enablement
 Automatic risk creation	 Proactive and incremental updates & event notifications	 Unified risk register ensures efficiency & consistency	 Speed communications with workflows & ticketing	 Rules & actions library
 Exec & ops dashboards	 Continuous business scoring from 200k+ sources	 Inherent & residual risk tracking	 Share risk intel: research, assessments & external feeds	 Vendor attribute & events support
 Comments & tagging	 Member intelligence sharing & benchmarking	 Auto-flagging recommendations	 Consolidate, quantify and analyze threat intelligence	 Extensible engine
		 Automated risk reviews	 Report across security, compliance and privacy	 Intelligent actions

Adopt using a Risk Operation Center (ROC) for support



The Old Way: Point-Solution Mindset

- ◆ Reactive
- ◆ Focus on Individual Controls
- ◆ Fragmented and inefficient
- ◆ Spend a lot and not necessarily improve security

The New Way: Holistic Security Mindset

- ◆ Proactive
- ◆ Focus on Total Solutions
- ◆ Gap-Based & Risk-Based
- ◆ Spend less and improve security more



The Holistic Picture Risk Intelligence from Every Corner

Public Sources

Business & Breach Monitoring:

- Data breach sites
- Corporate sites
- Regulatory portals
- Review websites
- Job boards
- Trade publications
- Industry sites
- News feeds
- And more

Vendor Community

- Proactive assessments
- Vendor Initiated Events
- Certifications
- Docs & agreements

Vendor Risk Intelligence

Continuous, Comprehensive, Relevant:

- Global research
- Assessments
- Partner feeds

Private Sources

Extended Profiles:

- Credit reports
- Risk scores
- Financials
- Payments
- Legal Actions
- Certifications

Cyber Monitoring:

- 65+ threat feeds
- 50+ paste sites
- Blogs & social media
- Code repositories
- 1.5k+ hacker forums
- Dark web (80+ forums)

Prevalent

Securing the
Extended Enterprise

Completed Assessments

- Networks & Exchanges
- Sig-Lite/Sig-Core
- Prevalent Compliance Framework (PCF)
- Cybersecurity Maturity Model Compliance (CMMC)

Regulatory Monitoring

Coverage across regulations and frameworks:

- CCPA
- NYDFS
- GDPR
- ISO
- NIST
- CMMC
- HIPAA
- PCI
- CAIQ
- And more

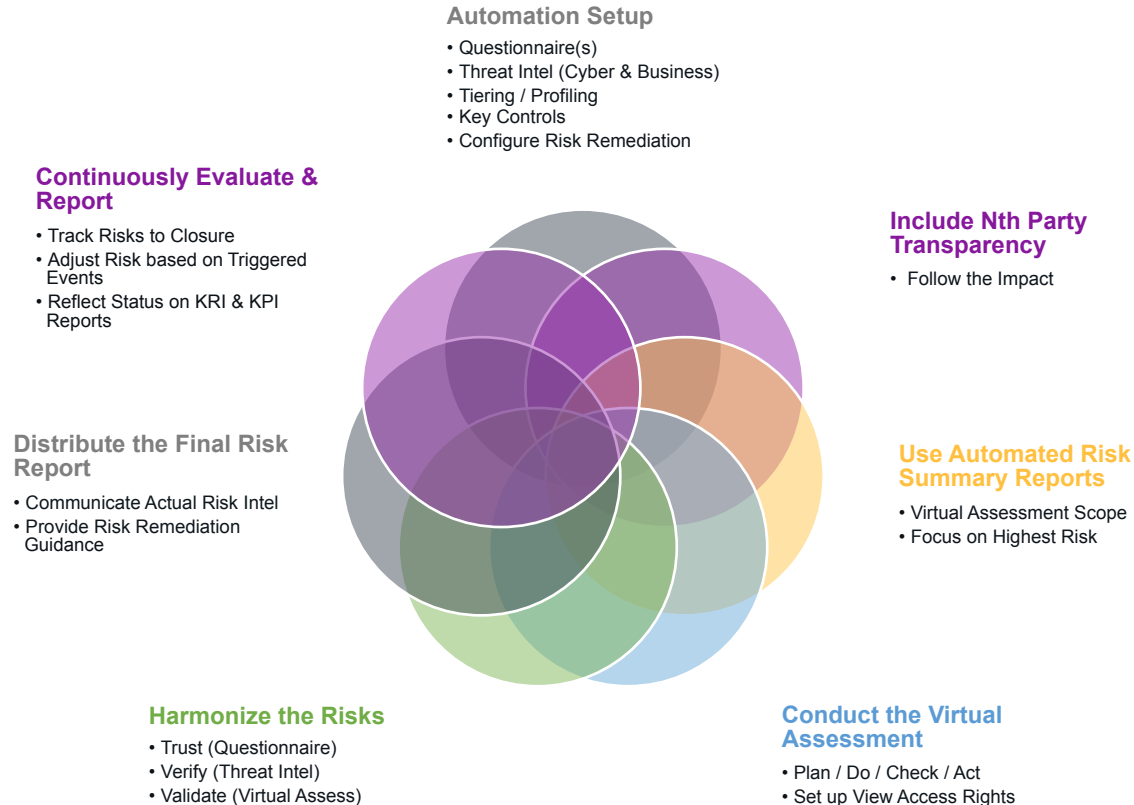
Technology Integrations

- ServiceNow
- RSA Archer
- BitSight
- And more

Industry Partnerships

- H-ISAC
- LVN
- Shared Assessments
- Legal Theorem

Risk Validation in a Virtual Only World



Questions?



info@prevalent.net



Follow Prevalent on LinkedIn



Follow Prevalent on Twitter



info@asmgi.com



Follow ASMGi on LinkedIn



Follow ASMGi on Twitter

