# Stop, Spot, & Defend

# Aligning Enterprise Architecture with Cybersecurity

ABACUS

Hosted by Kishan Patel

avolution

www.avolutionsoftware.com

# avolution ABACUS

**21** YEARS
LEADING ENTERPRISE ARCHITECTURE

**OFFICES**
WORLDWIDE

**LEADER IN**
GARTNER MQ & FORRESTER WAVE
#1 Independent Tool Reviews

**THOUSANDS**
OF ABACUS USERS

IN OVER
**100**
COUNTRIES


Kishan Patel

*Software Consultant, Avolution*


Supporting over 100+ frameworks and notations incl. TOGAF, ArchiMate, BPMN, ACORD, BIAN

avolution ABACUS

Sections

KIRO 7 LIVE. LOCAL. IN-DEPTH.

News • Weather • Video • Jesse Jones • Gets Real • Traffic • Sports • Apps & New

WEATHER ALERT | Flood Warning

# In 2021, the data breaches just keep on coming

SECURITY

MAGAZINE NEWS COLUMNS MANAGEMENT PHYSICAL

EDUCATION: UNIVERSITY

HOSPITALS & MEDICAL CENTERS

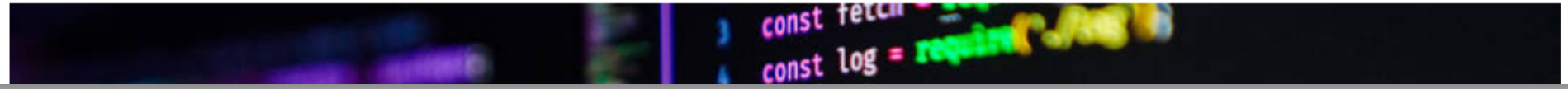
CRITICAL INFRASTRUCTURE

MORE

Home » US expected to break data breach record in 2021

Cyber | Security Newswire | Security Leadership and Management | Cyb | Government: Federal, State and Local

# US expected to break data breach record in 2021






avolution ABACUS

THE WHITE HOUSE

BRIEFING ROOM

# FACT SHEET: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure

JULY 28, 2021 • STATEMENTS AND RELEASES

The Biden Administration continues to take steps to safeguard U.S. critical infrastructure from growing, persistent, and sophisticated cyber threats

# Cybersecurity — Executive Order 13636

On February 12, 2013, President Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The Executive Order is designed to increase the level of core capabilities for our critical infrastructure to manage cyber risk. It does this by focusing on three key areas: (1) information sharing, (2) privacy, and (3) the adoption of cybersecurity practices.

The EO tasked the National Institute for Standards and Technology (NIST) to work with the private sector to identify existing voluntary consensus standards and industry best practices and build them into a Cybersecurity Framework. The Administration recognizes that there are private-sector cyber leaders who are already

EO

Cyb

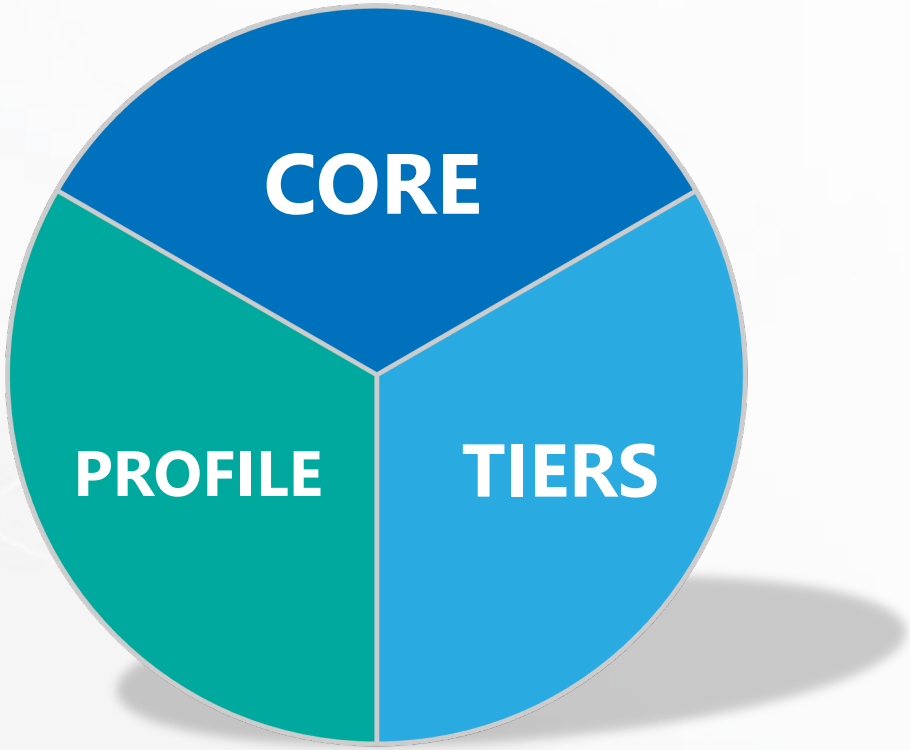
For

avolution ABACUS

# What is NIST?

NIST is a Cybersecurity Framework that helps organizations improve their cybersecurity programs.

The framework consists of **3 key components**:




avolution ABACUS

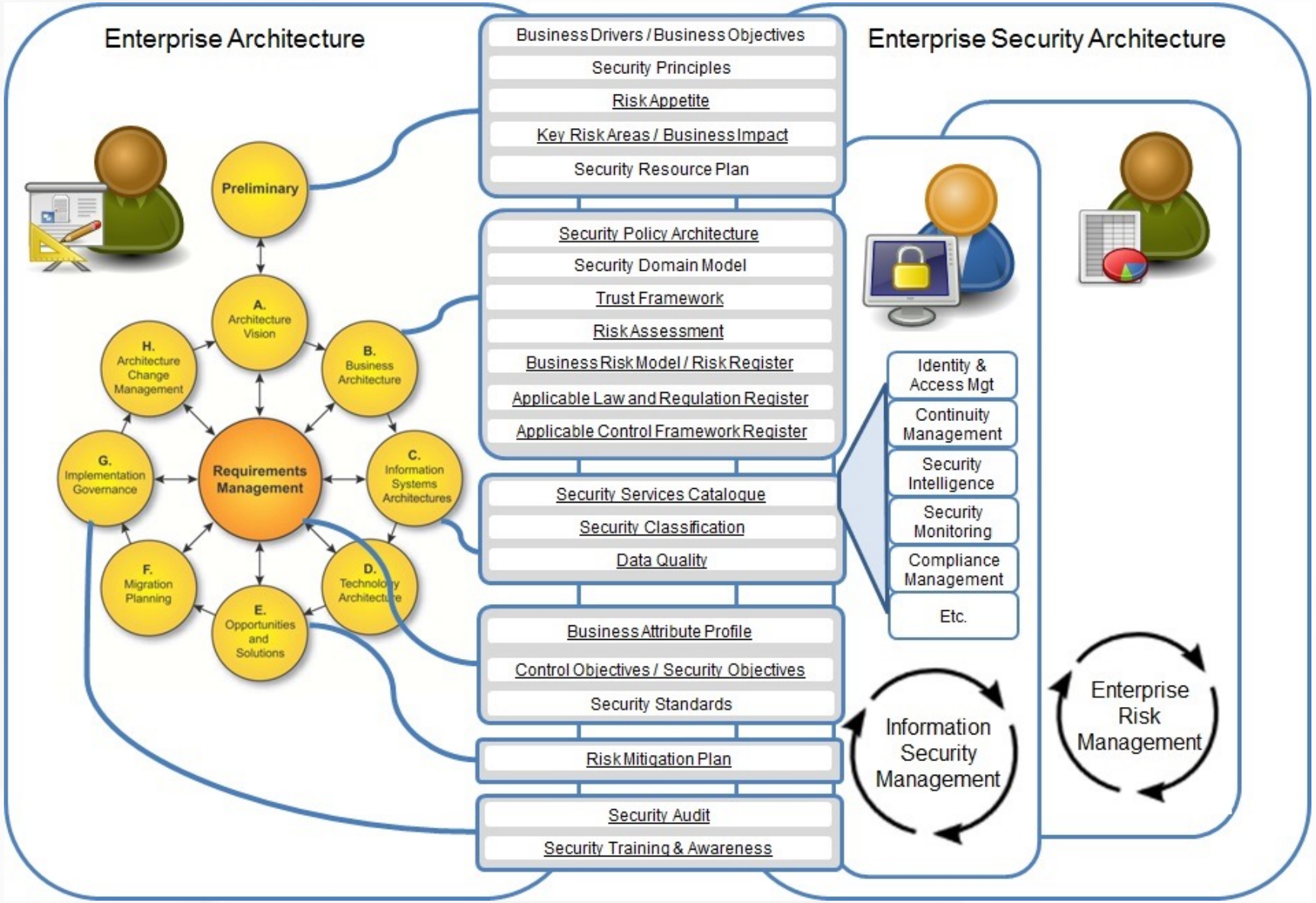
- Executive Order - Improving the Nation's Cybersecurity
- Stakeholder Engagement
- Computer Security Resource Center
- Cybersecurity Framework
- Privacy Framework
- Risk Management Framework
- Measurements for Information Security
- Cybersecurity Insights Blog
- National Cybersecurity Center of Excellence
- National Initiative for Cybersecurity Education (NICE)
- Small Business Cybersecurity Corner
- Ransomware Resources

- All Topics
- Advanced communications
- Artificial intelligence
- Bioscience
- Buildings and construction
- Chemistry
- Climate
- Cybersecurity
- Electronics
- Energy
- Environment
- Fire
- Forensic science
- Health
- Information technology
- Infrastructure
- Manufacturing
- Materials
- Mathematics and statistics


avolution ABACUS

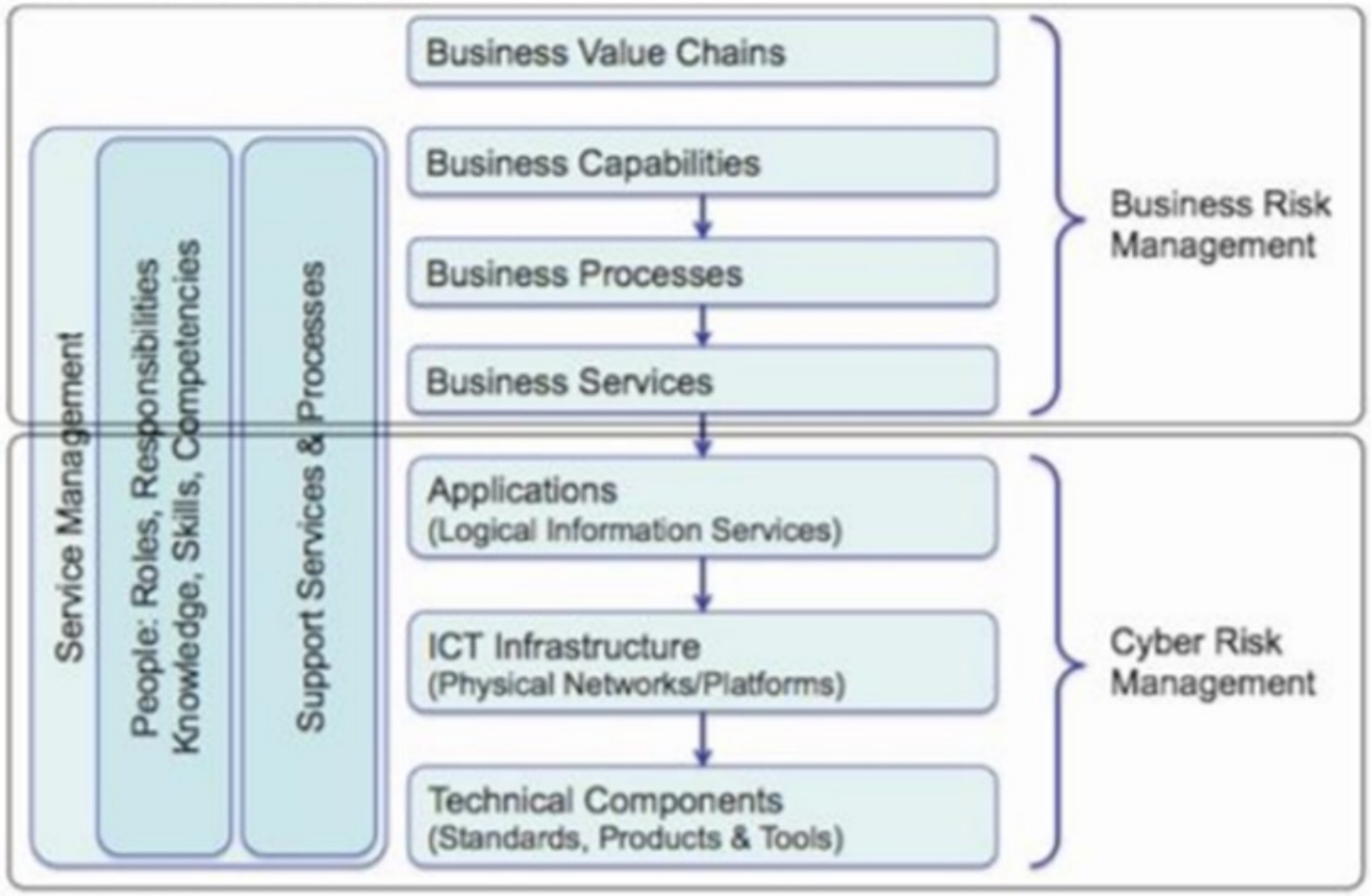
# STOP

How is your organization currently addressing cybersecurity concerns?




avolution ABACUS

# Business Stack



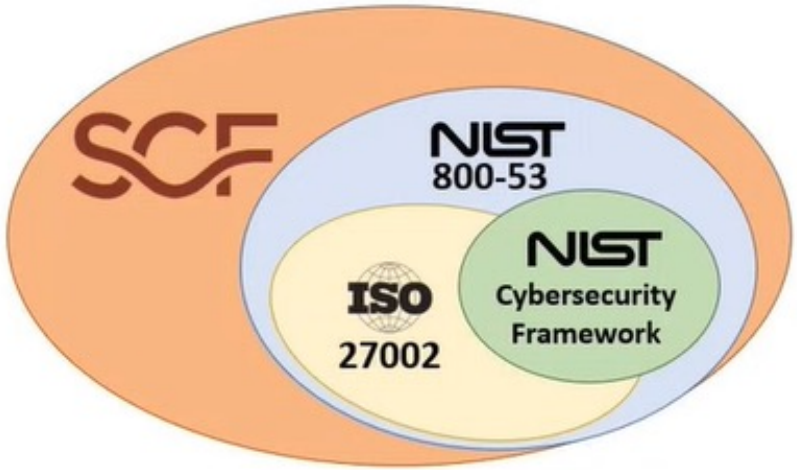


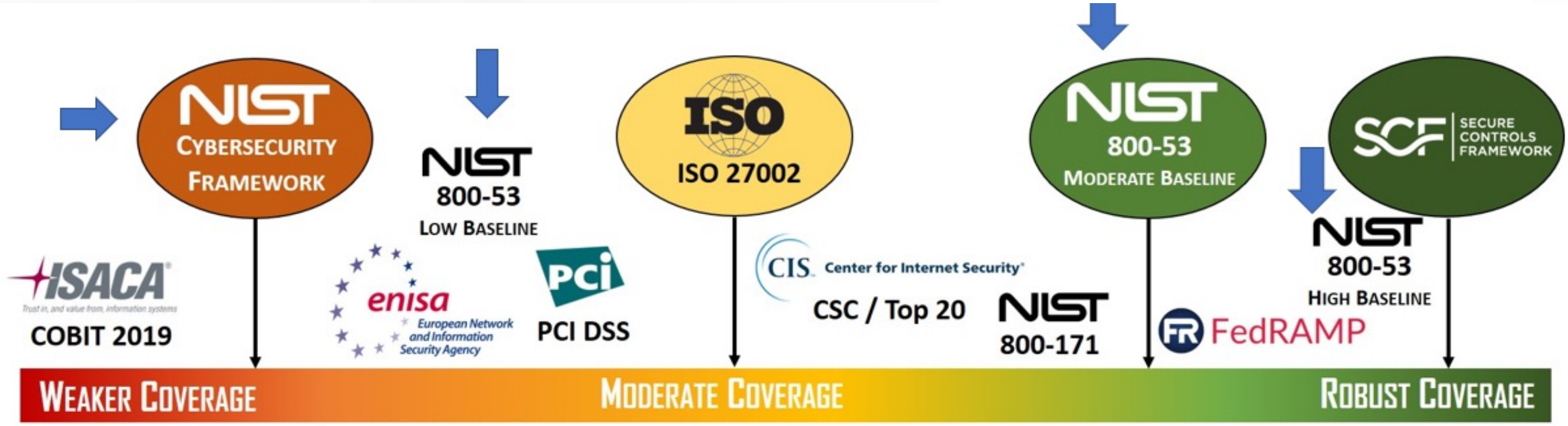

avolution ABACUS

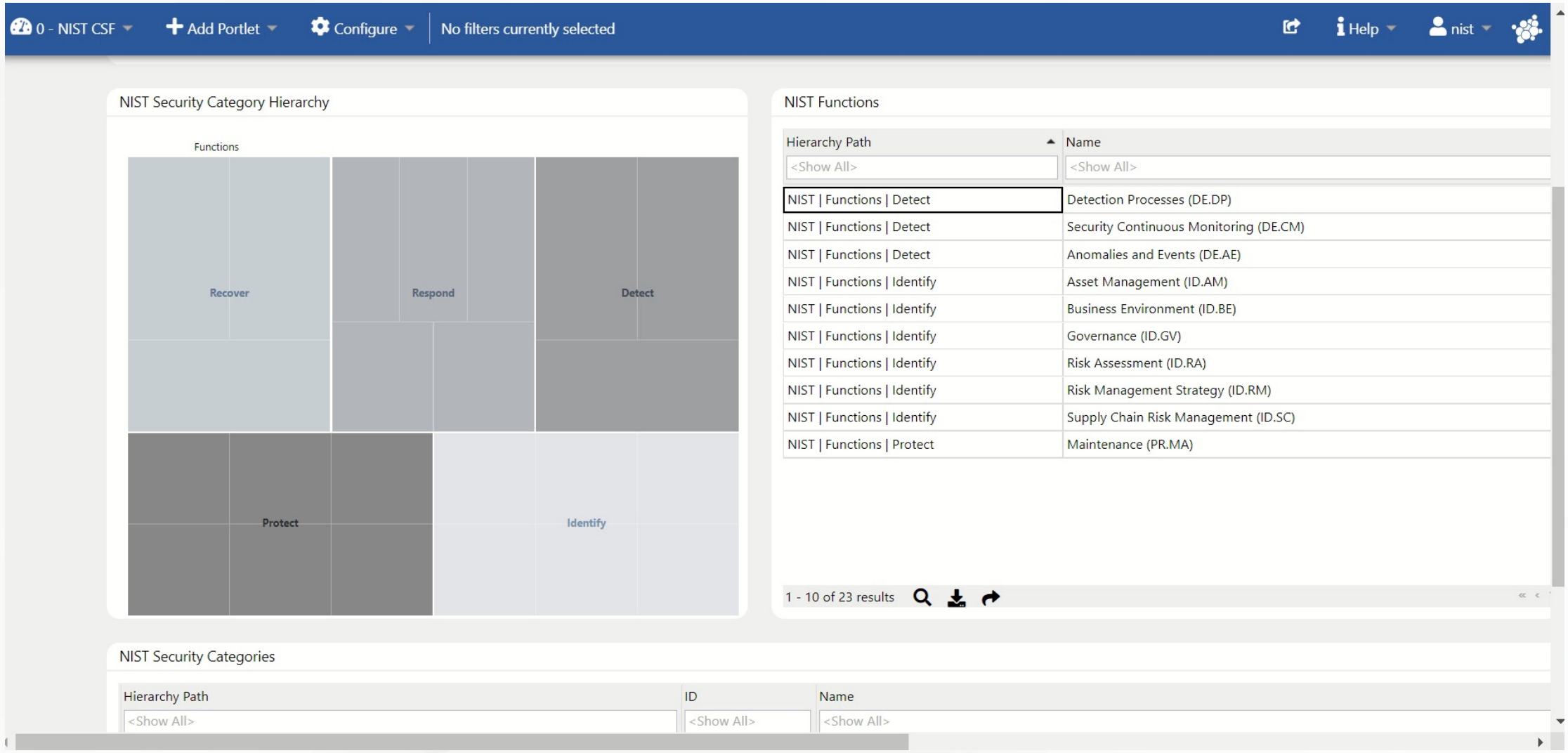
| ADM | Requirements | Risk Analysis Method | Control |
|---|---|---|---|
| Preliminary | To define approach and methods in accordance with customer or program | | Risk Management |
| Vision | To define the risk landscape to a program or enterprise requirements | Strategic Threat Scenarios, Risk Spectrum | |
| Business Architecture | To formalize the risk model defined in the vision stage against the business and the application at later stages | Tactical Threat Scenarios | |
| Information System Architecture | To apply to information arch | FAIR, SANS, ISO, **NIST**, OCTAVE | |
| Technology Architecture | To apply to tech arch | FAIR, SANS, ISO, **NIST**, OCTAVE | |
| Opportunities & Solution | To check and agree risk | FAIR, SANS, ISO, **NIST**, OCTAVE | |
| Migration Planning | Program Management RISK | CRAMM, ARM | |
| Implementation Governance | Program Management RISK | CRAMM, ARM | |
| EA Change Management | Program Management RISK | Scenarios, CRAMM, ARM | |

# NIST CSF vs NIST 800-53

- NIST CSF provides a **flexible framework** that **any organization** can use for creating and managing a cybersecurity program
- NIST 800-53 provides **security controls** for implementing NIST CSF. NIST 800-53 **aids federal agencies** and entities doing business with them






avolution ABACUS

# Mapping NIST CSF to NIST 800-53 r5

| NIST CSF | | | NIST SP 800-53 |
|---|---|---|---|
| **Function** | **Category** | **Subcategory** | **NIST SP 800-53, Revision 5 Control** |
| **Identify (ID)** | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | **ID.AM-1:** Physical devices and systems within the organization are inventoried | CM-8, PM-5 |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | CM-8 |
| | | **ID.AM-3:** Organizational communication and data flows are mapped | AC-4, CA-3, CA-9, PL-8, SA-17 |
| | | **ID.AM-4:** External information systems are catalogued | AC-20, PM-5, SA-9 |
| | | **ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | CP-2, RA-2, RA-9, SA-20, SC-6 |
| | | **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third party stakeholders (e.g., suppliers, customers, partners) are established | CP-2, PS-7, PM-2, PM-29 |

Function | Category | Subcategory

Control Family | Control

avolution ABACUS

# SPOT

Create a baseline assessment

Conduct a risk assessment

# Risk Assessment

## Two levels of risk in the TOGAF Standard:

- **Initial Level of Risk:** risk categorization prior to determining and implementing mitigating actions
- **Residual Level of Risk:** risk categorization after implementation of mitigating actions (if any)



avolution ABACUS

| Corporate Risk Impact Assessment | | | | | |
|---|---|---|---|---|---|
| Effect | Frequency | | | | |
| | Frequent | Likely | Occasional | Seldom | Unlikely |
| Catastrophic | E | E | H | H | M |
| Critical | E | H | H | M | L |
| Marginal | H | M | M | L | L |
| Negligible | M | L | L | L | L |



*Figure 27-1: Risk Classification Scheme*

- **Extremely High Risk (E):** the transformation effort will most likely fall with severe consequences
- **High Risk (H):** significant failure of parts of the transformation effort resulting in certain goals not being achieved
- **Moderate Risk (M):** noticeable failure of parts of the transformation effort threatening the success of certain goals
- **Low Risk (L):** certain goals will not be wholly successful

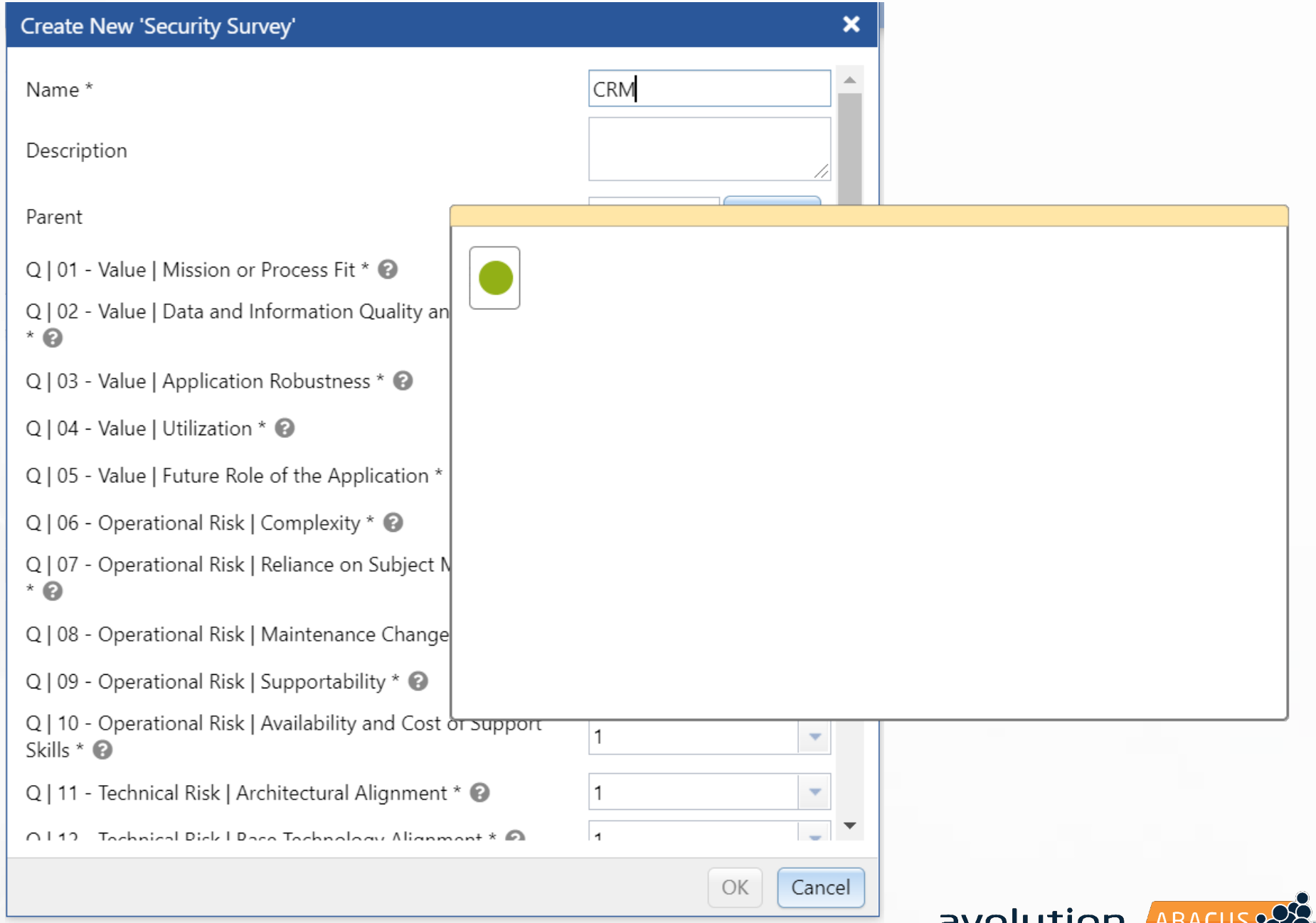
# Risk Impact Matrix

Risk

Drag a column header here to group by that column.

| Name | Effect(Preliminary Risk) | Frequency(Preliminary Risk) | Impact(Preliminary Risk) | Mitigation | Effect(Residual Risk) | Frequency(Residual Risk) | Impact(Residual Risk) |
|---|---|---|---|---|---|---|---|
| (All) | (All) | (All) | (All) | (All) | (All) | (All) | (All) |
| Vulnerability in applications | Catastrophic | Unlikely | Moderate Risk | Implement vulnerability management program and application firewalls | Critical | Unlikely | Low Risk |
| Technology goes out of support due to lack of supplier management | Critical | Unlikely | Low Risk | Populate Suppliers into the EA repository | Marginal | Unlikely | Low Risk |
| Supplier XYZ Pty Ltd stability | Critical | Seldom | Moderate Risk | Conduct due diligence on XYZ Pty Ltd | Marginal | Unlikely | Low Risk |
| Not having a proper disaster recovery plan for applications | Catastrophic | Occasional | High Risk | Build a disaster recovery environment for the applications | Critical | Unlikely | Low Risk |
| Losing customers due to the pasts 'swivel chair' integration policy | Critical | Likely | High Risk | Single Customer View project | Marginal | Seldom | Low Risk |
| Lose #1 market position due to lack of investment | Marginal | Occasional | Moderate Risk | Look at industry benchmarks for investment | Marginal | Seldom | Low Risk |
| Lack of segregation of duties (SoD) | Marginal | Seldom | Low Risk | Implement SoD for the areas needed | Negligible | Seldom | Low Risk |
| Lack of Access Control | Critical | Seldom | Moderate Risk | Establish network access controls | Marginal | Unlikely | Low Risk |
| ERP performance causes employee churn | Marginal | Likely | Moderate Risk | ERP Tech Refresh and Financials Decommissioning projects | Negligible | Seldom | Low Risk |
| DDOS Attack | Catastrophic | Unlikely | Moderate Risk | Continuously monitor network traffic | Critical | Unlikely | Low Risk |

avolution ABACUS

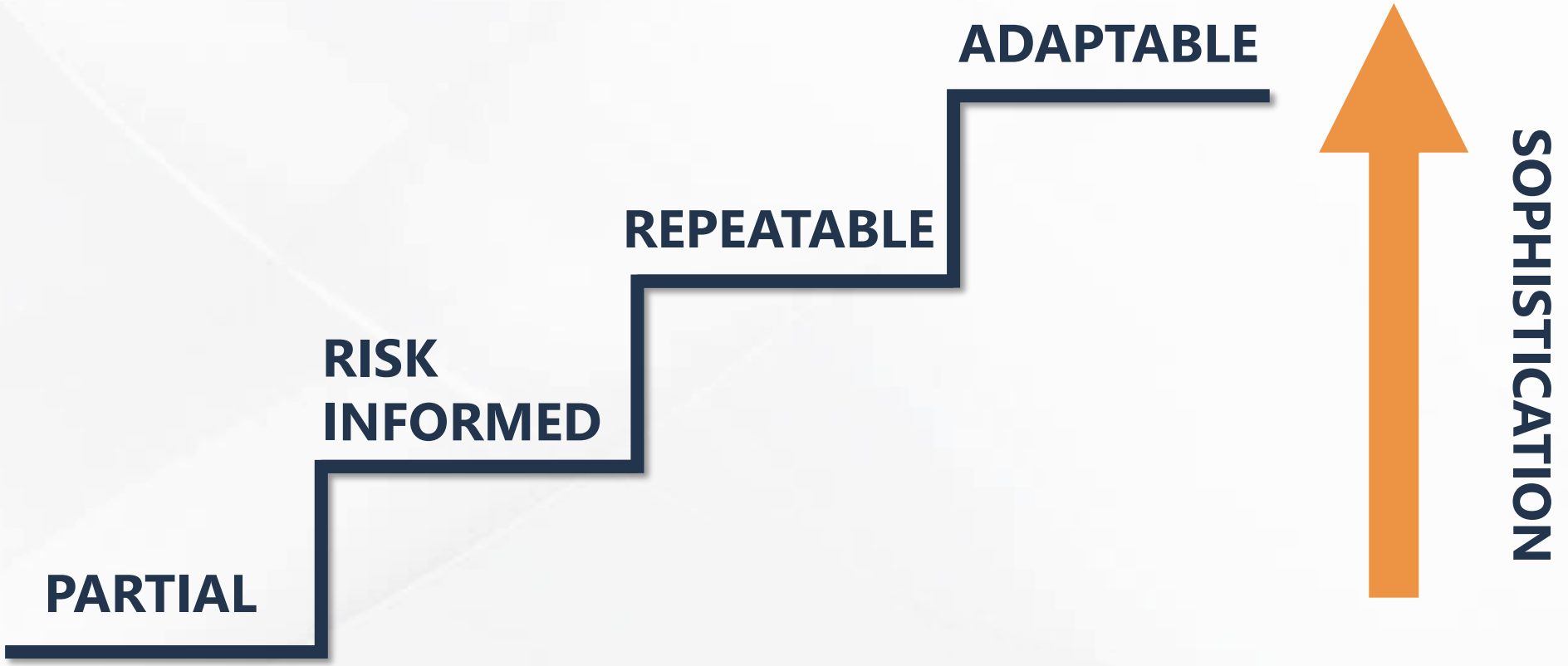



avolution ABACUS

| NIST Categories (All) | Objectives (All) | Priority Baseline (All) | Priority Target (All) | Scored Gap (-... <> 0 |
|---|---|---|---|---|
| Physical devices and systems within the organization are inventoried | 7: Pass Required Au... | Tier 2 | Tier 3 | 5 |
| The organization's role in the supply chain is identified and communicated | 2: Maintain Environm... | Tier 1 | Tier 2 | 4 |
| The organization's place in critical infrastructure and its industry sector is... | 3: Maintain Operation... | Tier 1 | Tier 2 | 4 |
| The organization's role in the supply chain is identified and communicated | 4: Maintain Prepared... | Tier 2 | Tier 3 | 5 |
| Asset vulnerabilities are identified and documented | 2: Maintain Environm... | Tier 1 | Tier 2 | 4 |
| Asset vulnerabilities are identified and documented | 3: Maintain Operation... | Tier 1 | Tier 4 | 4 |
| Threats, both internal and external, are identified and documented | 1: Maintain Personnel... | Tier 2 | Tier 4 | 5 |
| Recovery activities are communicated to internal and external stakehold... | 1: Maintain Personnel... | Tier 1 | Tier 3 | 9 |
| Organizational cybersecurity policy is established and communicated | 2: Maintain Environm... | Tier 1 | Tier 3 | 9 |
| Governance and risk management processes address cybersecurity risks | 1: Maintain Personnel... | Tier 2 | Tier 3 | 5 |
| Governance and risk management processes address cybersecurity risks | 2: Maintain Environm... | Tier 1 | Tier 3 | 9 |
| Legal and regulatory requirements regarding cybersecurity,including priv... | 5: Maintain Quality of... | Tier 1 | Tier 3 | 9 |
| Governance and risk management processes address cybersecurity risks | 5: Maintain Quality of... | Tier 1 | Tier 4 | 4 |
| Risk responses are identified and prioritized | 2: Maintain Environm... | Tier 1 | Tier 2 | 4 |
| Threats, vulnerabilities, likelihoods, and impacts are used to determine ri... | 4: Maintain Prepared... | Tier 2 | Tier 3 | 5 |
| Threats, vulnerabilities, likelihoods, and impacts are used to determine ri... | 7: Pass Required Au... | Tier 1 | Tier 4 | 9 |
| Risk management processes are established, managed, and agreed to b... | 3: Maintain Operation... | Tier 1 | Tier 3 | 9 |
| Risk management processes are established, managed, and agreed to b... | 8: Maintain Sensitive... | Tier 2 | Tier 3 | 5 |
| Organizational risk tolerance is determined and clearly expressed | 1: Maintain Personnel... | Tier 2 | Tier 3 | 5 |
| Public relations are managed | 6: Meet HR Requirem... | Tier 2 | Tier 3 | 5 |
| Response plan is executed during or after an incident | 6: Meet HR Requirem... | Tier 1 | Tier 3 | 9 |

# Framework Implementation Tiers

How cybersecurity risks and processes are viewed within organization




avolution ABACUS

Drag a column header here to group by that column.

| ID (All) | Name (All) | → Category (Refers to) (All) | Low BL (All) | Moderate BL (All) | High BL (All) | Total (local)... (All) |
|---|---|---|---|---|---|---|
| IR-4 | Incident Handling | Coordination with stakeholders... | True | True | True | 170 |
| CP-2 | Contingency Plan | Adequate capacity to ensure av... | True | True | True | 170 |
| CA-7 | Continuous Monitoring | Asset vulnerabilities are identifi... | True | True | True | 170 |
| SI-4 | System Monitoring | A baseline of network users an... | True | True | True | 170 |
| IR-8 | Incident Response Plan | Coordination with stakeholders... | True | True | True | 170 |
| PM-9 | Risk Management Strategy | Contracts with suppliers and thi... | False | False | False | 0 |
| CA-2 | Control Assessments | Asset vulnerabilities are identifi... | True | True | True | 170 |
| RA-3 | Risk Assessment | A vulnerability managementpla... | True | True | True | 170 |
| SA-14 | Criticality Analysis | Dependencies and critical funct... | False | False | False | 0 |
| AU-6 | Audit Record Review, Analysis, and Reporting | Audit/log records are determine... | True | True | True | 170 |
| RA-5 | Vulnerability Monitoring and Scanning | A vulnerability managementpla... | True | True | True | 170 |
| SA-9 | External System Services | Contracts with suppliers and thi... | True | True | True | 170 |
| SA-12 | Supply Chain Protection | A System Development Life Cy... | False | False | False | 0 |
| PE-3 | Physical Access Control | Detection processes are tested... | True | True | True | 170 |
| PM-14 | Testing, Training, and Monitoring | Detection activities comply with... | False | False | False | 0 |
| PM-11 | Mission and Business Process Definition | Cybersecurity roles and respon... | False | False | False | 0 |
| PS-7 | External Personnel Security | Cybersecurity is included in hu... | True | True | True | 170 |
| AU-12 | Audit Record Generation | Audit/log records are determine... | True | True | True | 170 |
| SI-5 | Security Alerts, Advisories, and Directives | Asset vulnerabilities are identifi... | True | True | True | 170 |
| AC-4 | Information Flow Enforcement | A baseline of network users an... | False | True | True | 138 |
| RA-2 | Security Categorization | Potential business impacts and... | True | True | True | 170 |

| Name (All) | Availability(Security... (All) | Confidentiality(Security... (All) | Integrity(Security... (All) | Security Category (All) | → Control (Employ) (All) |
|---|---|---|---|---|---|
| .NET Memory Profiler | Low | Moderate | High | High-impact | Automated Notificatior |
| 1Password | High | High | Low | High-impact | Automated Notificatior |
| 7-Zip | High | Moderate | Moderate | High-impact | Automated Notificatior |
| ABACUS (Studio in the)... | Moderate | Moderate | High | High-impact | Automated Notificatior |
| ABACUS Analytics Engine | Low | Low | Low | Low-impact | Fire Protection, Inside |
| ABACUS Enterprise | Not Applicable | Low | Moderate | Moderate-impact | Continuous Learning C |
| ABACUS Studio | Moderate | Moderate | Moderate | Moderate-impact | Continuous Learning C |
| Actipro UI Studio | High | Low | Low | High-impact | Automated Notificatior |
| Actipro WPF docking &... | Moderate | Moderate | Low | Moderate-impact | Continuous Learning C |
| AddThis | Moderate | Low | Moderate | Moderate-impact | Continuous Learning C |
| Adobe Acrobat | Low | Low | Moderate | Moderate-impact | Continuous Learning C |
| Adobe Illustrator | Low | High | Moderate | High-impact | Automated Notificatior |
| Adobe Media Encoder 20... | Moderate | Moderate | Low | Moderate-impact | Continuous Learning C |
| Adobe Photoshop | Low | Low | Low | Low-impact | Fire Protection, Inside |
| Adobe Premiere Pro | Moderate | Low | High | High-impact | Automated Notificatior |
| Adobe Premiere Rush | Low | Moderate | Moderate | Moderate-impact | Continuous Learning C |
| Alternet Code Editor | Low | High | Low | High-impact | Automated Notificatior |
| Archi | High | Moderate | Low | High-impact | Automated Notificatior |
| Atom | Moderate | Low | High | High-impact | Automated Notificatior |
| Automatic ABACUS Stud... | Low | Low | Moderate | Moderate-impact | Continuous Learning C |
| AWS Command Line Inte... | Low | Moderate | Low | Moderate-impact | Continuous Learning C |

# Security Objectives

## Availability:

Ensuring timely and reliable access to and use of information

*A loss of availability is the **disruption of access to or use of information** or an information systems*

- LOW: The disruption of access to or use of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals
- MODERATE: The disruption of access to or use of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals
- HIGH: The disruption of access to or use of information could be expected to have **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals

## Confidentiality:

Preserving authorized restrictions on information access and disclosure, incl means for protecting personal privacy & proprietary information.

*A loss of confidentiality is the **unauthorized disclosure of information.***

- LOW: The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals
- MODERATE: The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals
- HIGH: The unauthorized disclosure of information could be expected to have **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals

## Integrity:

Guarding against improper information modification or destruction and includes ensuring information non-repudiation & authenticity

*A loss of integrity is the **unauthorized modification or destruction** of information.*

- LOW: The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals
- MODERATE: The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals
- HIGH: The unauthorized modification or destruction of information could be expected to have **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals

avolution ABACUS

| Name (All) | Availability(Security... (All) | Confidentiality(Security... (All) | Integrity(Security... (All) | Security Category (All) | → Control (Employ) (All) |
|---|---|---|---|---|---|
| Application 1 | Low | Moderate | High | High-impact | Automated Notificatior |
| Application 10 | Moderate | Low | Moderate | Moderate-impact | Continuous Learning C |
| Application 100 | High | Low | Low | High-impact | Automated Notificatior |
| Application 101 | Low | Low | Low | Low-impact | Fire Protection, Inside |
| Application 102 | Low | High | High | High-impact | Automated Notificatior |
| Application 103 | Moderate | Moderate | Moderate | Moderate-impact | Continuous Learning C |
| Application 104 | Low | Moderate | Moderate | Moderate-impact | Continuous Learning C |
| Application 105 | High | Low | Low | High-impact | Automated Notificatior |
| Application 106 | Moderate | Low | Low | Moderate-impact | Continuous Learning C |
| Application 107 | Low | Moderate | Moderate | Moderate-impact | Continuous Learning C |
| Application 108 | Low | Low | Low | Low-impact | Fire Protection, Inside |
| Application 109 | Moderate | Low | Low | Moderate-impact | Continuous Learning C |
| Application 11 | Low | Low | Moderate | Moderate-impact | Continuous Learning C |
| Application 110 | Low | Moderate | Moderate | Moderate-impact | Continuous Learning C |
| Application 111 | Moderate | Low | Low | Moderate-impact | Continuous Learning C |
| Application 112 | Low | Moderate | Moderate | Moderate-impact | Continuous Learning C |
| Application 113 | Low | Low | Low | Low-impact | Fire Protection, Inside |
| Application 114 | High | Low | Low | High-impact | Automated Notificatior |
| Application 115 | Moderate | High | High | High-impact | Automated Notificatior |
| Application 116 | Moderate | Low | Low | Moderate-impact | Continuous Learning C |
| Application 117 | Low | Moderate | Moderate | Moderate-impact | Continuous Learning C |

# DEFEND

## Analysis and Monitoring
## Gap Analysis

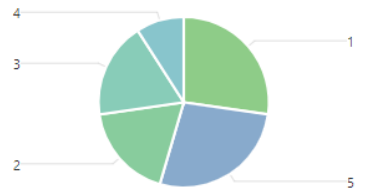
# Analysis and Monitoring

Risk Register

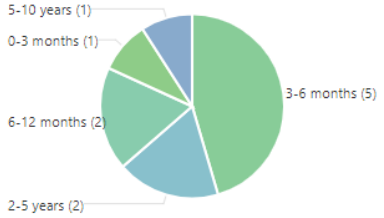
| Approach | Name | Validation | Priority | Probability | Impact | ← Department (Impacted By) | Identified date |
|---|---|---|---|---|---|---|---|
| Mitigate | Losing customers due to the pasts 'swivel chair' integration policy | Validated | Medium-Low | 2 | 2 | AU-Sales & Marketing (10) | 01 Jan 2011 |
| Mitigate | ERP performance causes employee churn | Validated | Medium | 3 | 2 | AU-Customer Service (7), AU-Human Resources (2) | 01 Apr 2015 |
| Watch | Supplier XYZ Pty Ltd stability | Validated | Medium | 1 | 4 | AU-Customer Service (7), AU-Risk & Financial Services (5), AU-Sales & Marketing (10) | 01 Jul 2016 |
| Accept | Technology goes out of support due to lack of supplier | Validated | Medium | 4 | 1 | AU-Strategy & Operations (5) | 01 Sep 2016 |

1 - 5 of 5 results

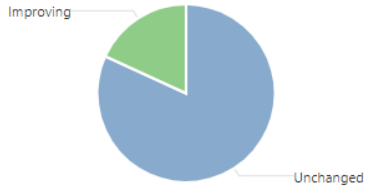
1) Identify | Impact (aggregated) on Risk in Production (As-Is)



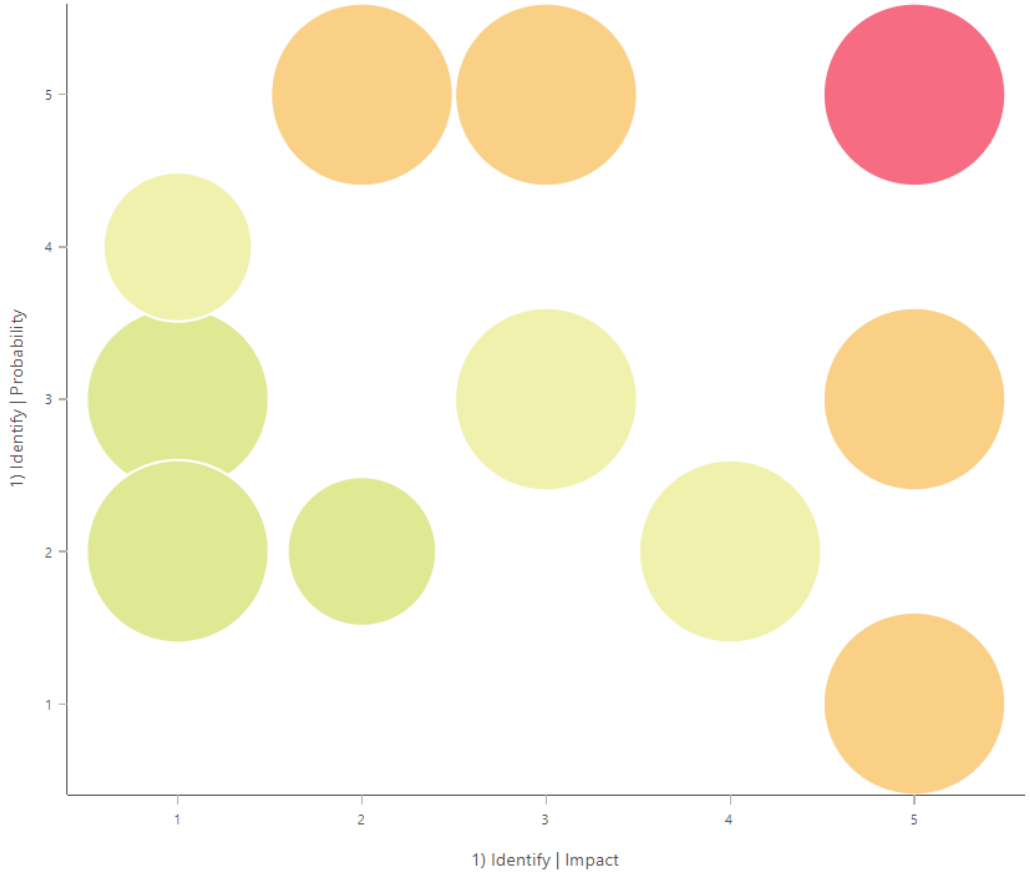

1) Identify | Timeframe (aggregated) on Risk in Production (As-Is)




4) Track | Trend (aggregated) on Risk in Production (As-Is)

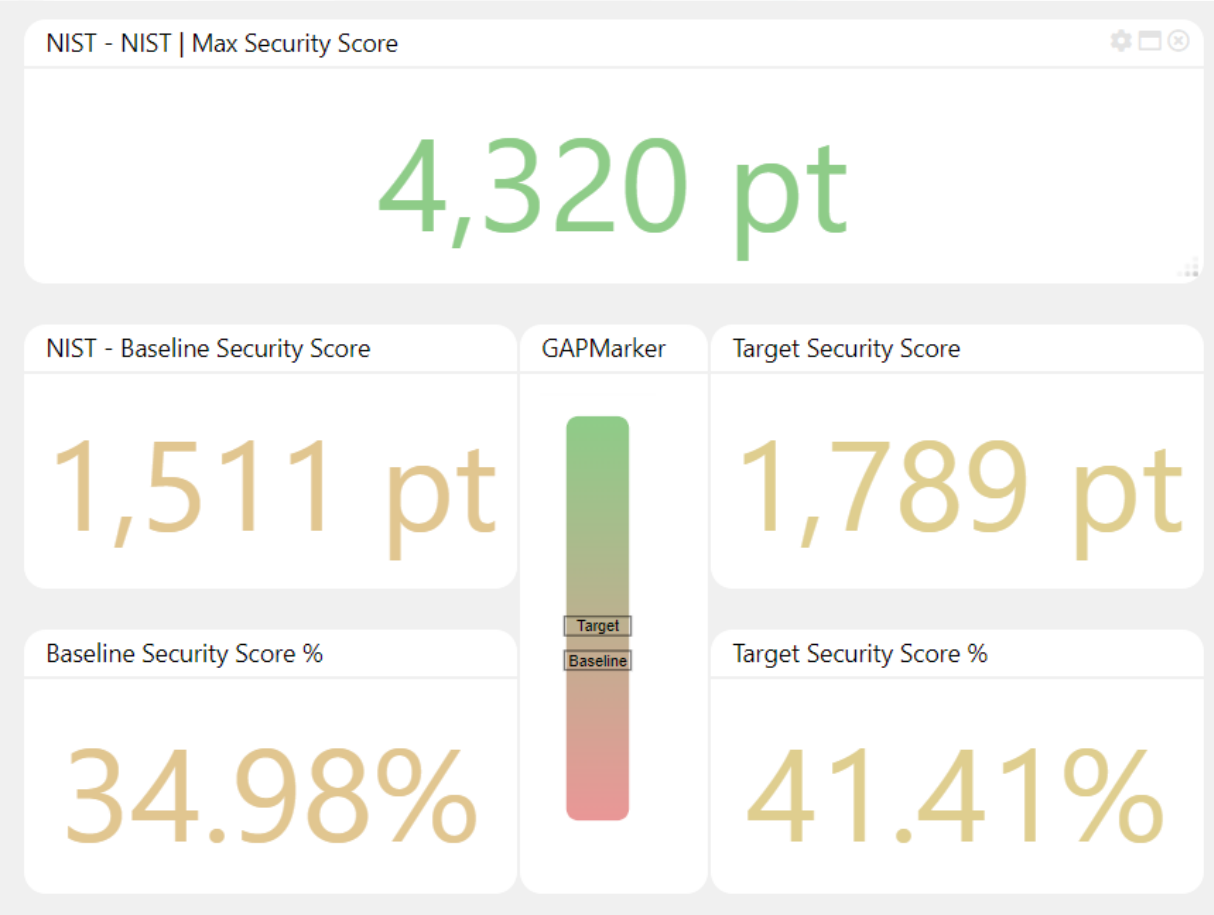



Size = Trend, Color = Priority




avolution ABACUS

# Gap Analysis




2.1 Mission Objectives Gap

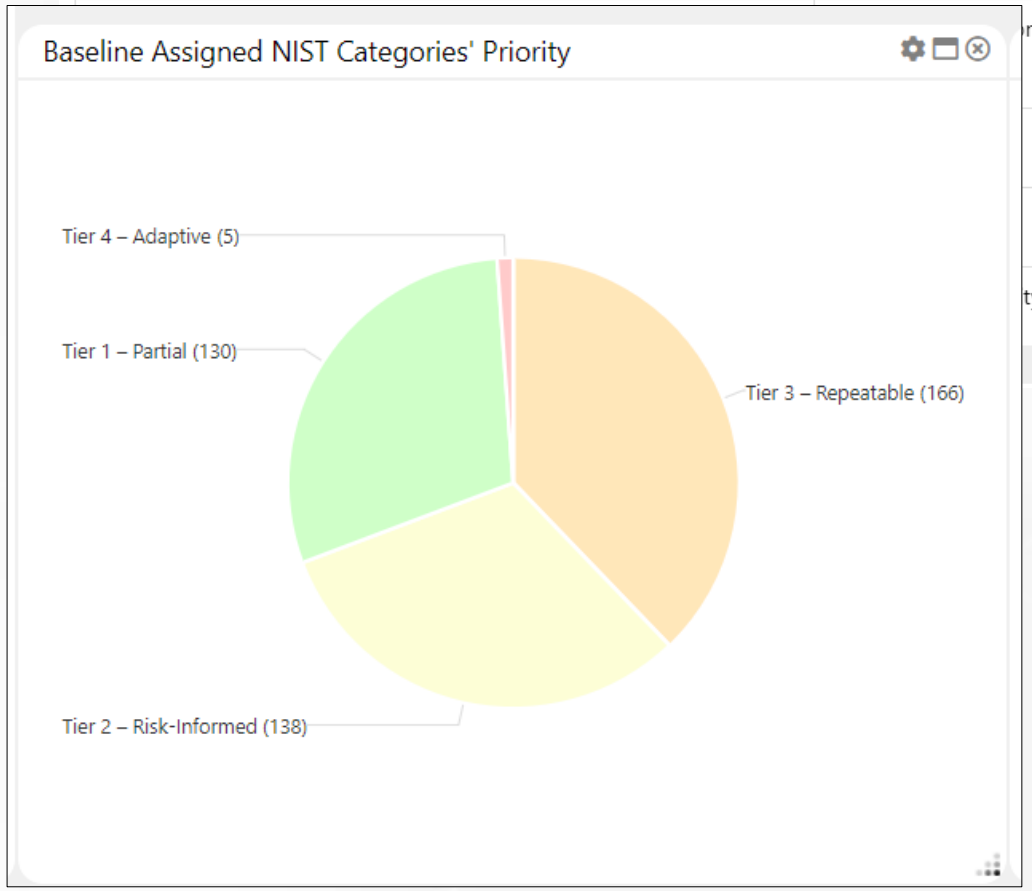
| Name | Baseline Security Score % | Target Security Score % | Security Score Gap % |
|---|---|---|---|
| <Show All> | <Show All> | <Show All> | <Show All> |
| 7: Pass Required Audits/Inspections | 32.22 | 40.74 | 8.52 |
| 3: Maintain Operational Security | 34.26 | 42.59 | 8.33 |
| 8: Maintain Sensitive Information | 34.63 | 42.04 | 7.41 |
| 2: Maintain Environmental Safety | 36.3 | 43.15 | 6.85 |
| 4: Maintain Preparedness | 36.85 | 43.7 | 6.85 |
| 5: Maintain Quality of Product | 32.59 | 37.96 | 5.37 |
| 1: Maintain Personnel Safety | 37.41 | 42.41 | 5 |
| 6: Meet HR Requirements | 35.56 | 38.7 | 3.14 |

1 - 8 of 8 results « ‹ 1 › » 10

avolution ABACUS

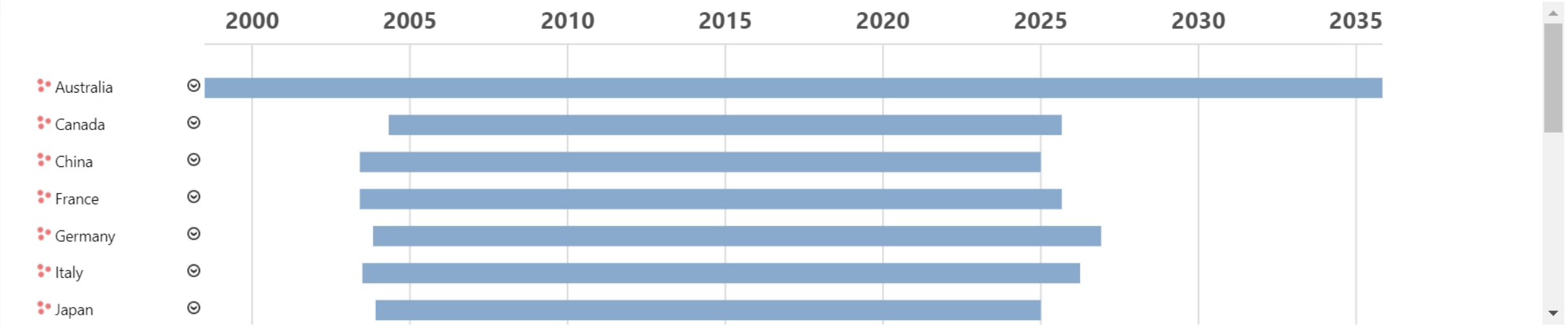
## 4. NIST Profile Current - Target

| NIST Categories | Objectives | Baseline Profile | Target Profile |
|---|---|---|---|
| <Show All> | <Show All> | <Show All> | <Show All> |
| Network integrity is protected (e.g., network segregation, network segmentation) | 7: Pass Required Audits/Inspections | Tier 1 – Partial | Tier 4 – Adaptive |
| A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) | 5: Maintain Quality of Product | Tier 1 – Partial | Tier 4 – Adaptive |
| | | Tier 1 – Partial | Tier 4 – Adaptive |
| | | Tier 1 – Partial | Tier 4 – Adaptive |
| | | Tier 1 – Partial | Tier 3 – Repeatable |
| | | Tier 1 – Partial | Tier 3 – Repeatable |

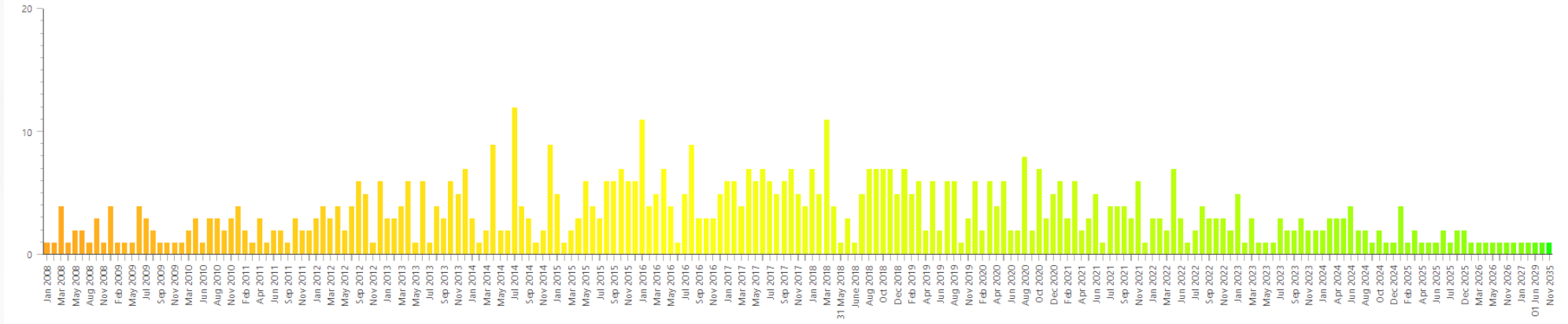



avolution ABACUS

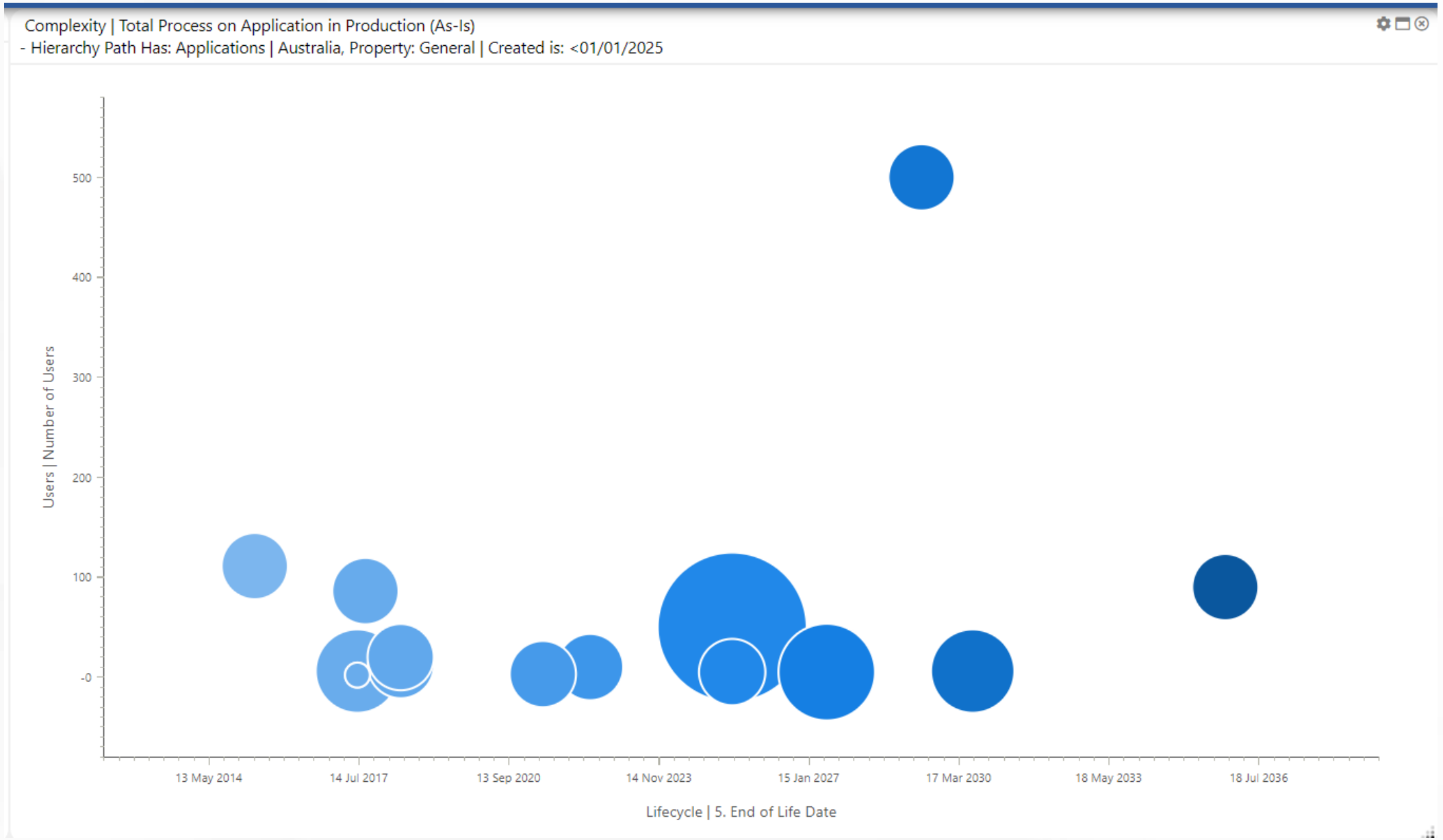
Gantt Chart



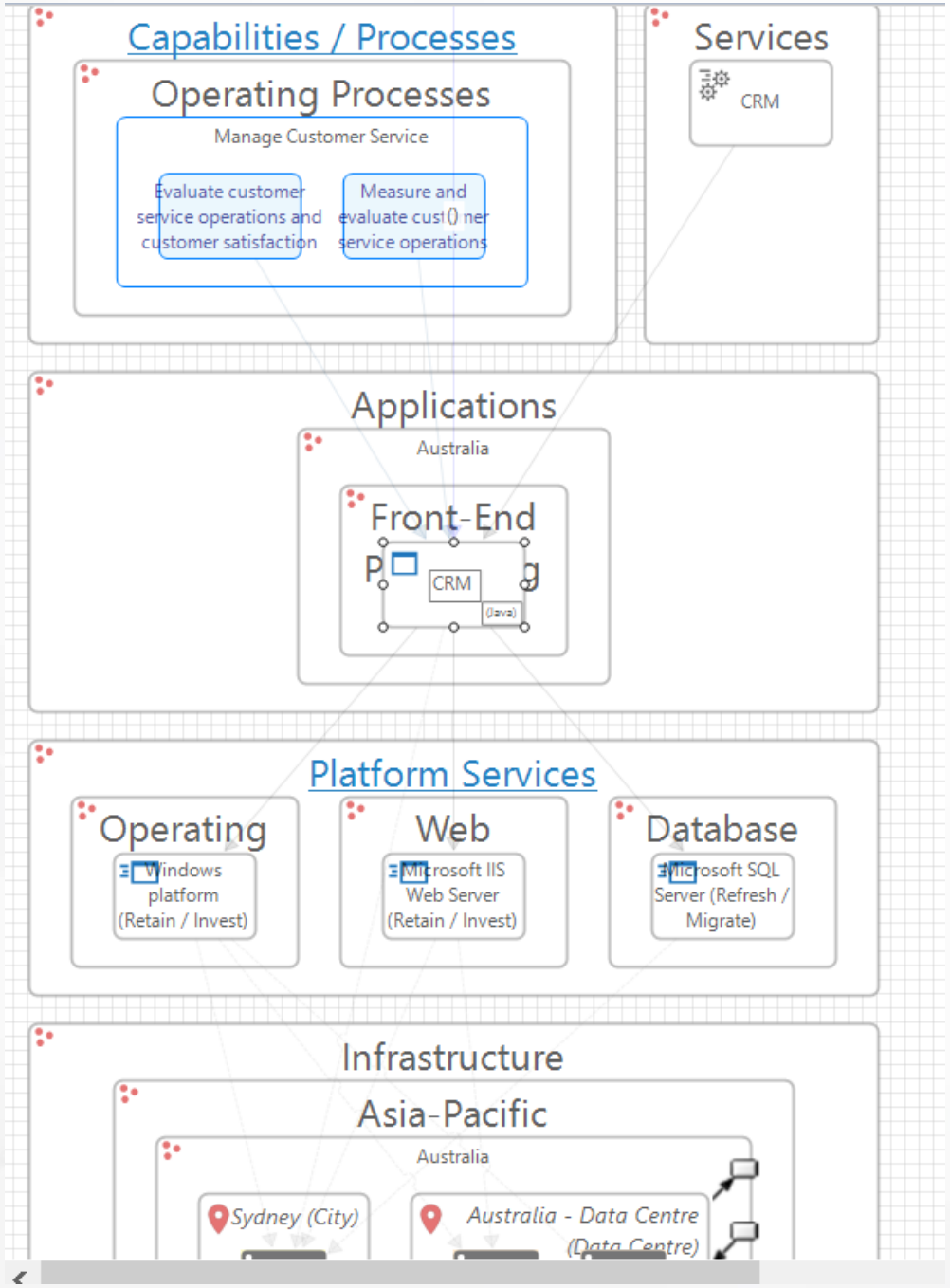

Lifecycle | 5. End of Life Date (aggregated) on Application in Production (As-Is)
- Property: Lifecycle | 5. End of Life Date is: >2007




avolution ABACUS




avolution ABACUS




avolution ABACUS

# Concluding Thoughts

- Cyber-risks are relevant at every level of the enterprise architecture
- Being proactive is necessary to stop cybersecurity failures before they happen
- TOGAF and NIST can be used together to provide robust cybersecurity coverage



avolution ABACUS

# Thank you!

# Thank you!

## Like some more information?

Visit out website:
https://www.avolutionsoftware.com

Join a Community!
LinkedIn, Twitter,
ABACUS Knowledge Portal

Visit our YouTube Channel
for more OG webinars and tutorials

Contact us:
abacus@avolutionsoftware.com
www.avolutionsoftware.com