intragen

IDENTITY SECURITY IN THE SPOTLIGHT

NIST CSF 2.0 and NIS2

Paul Cameron
Chief Revenue Officer
paul.cameron@intragen.com

INTRODUCTION TO NIST CSF 2.0

- Global Directive. NIS2 is the EU incarnation
- NIS2 EU states deadline 17th October 2024
- Applies to:
  - Essential Entities
  - Important Entities
  - Operators of critical facilities

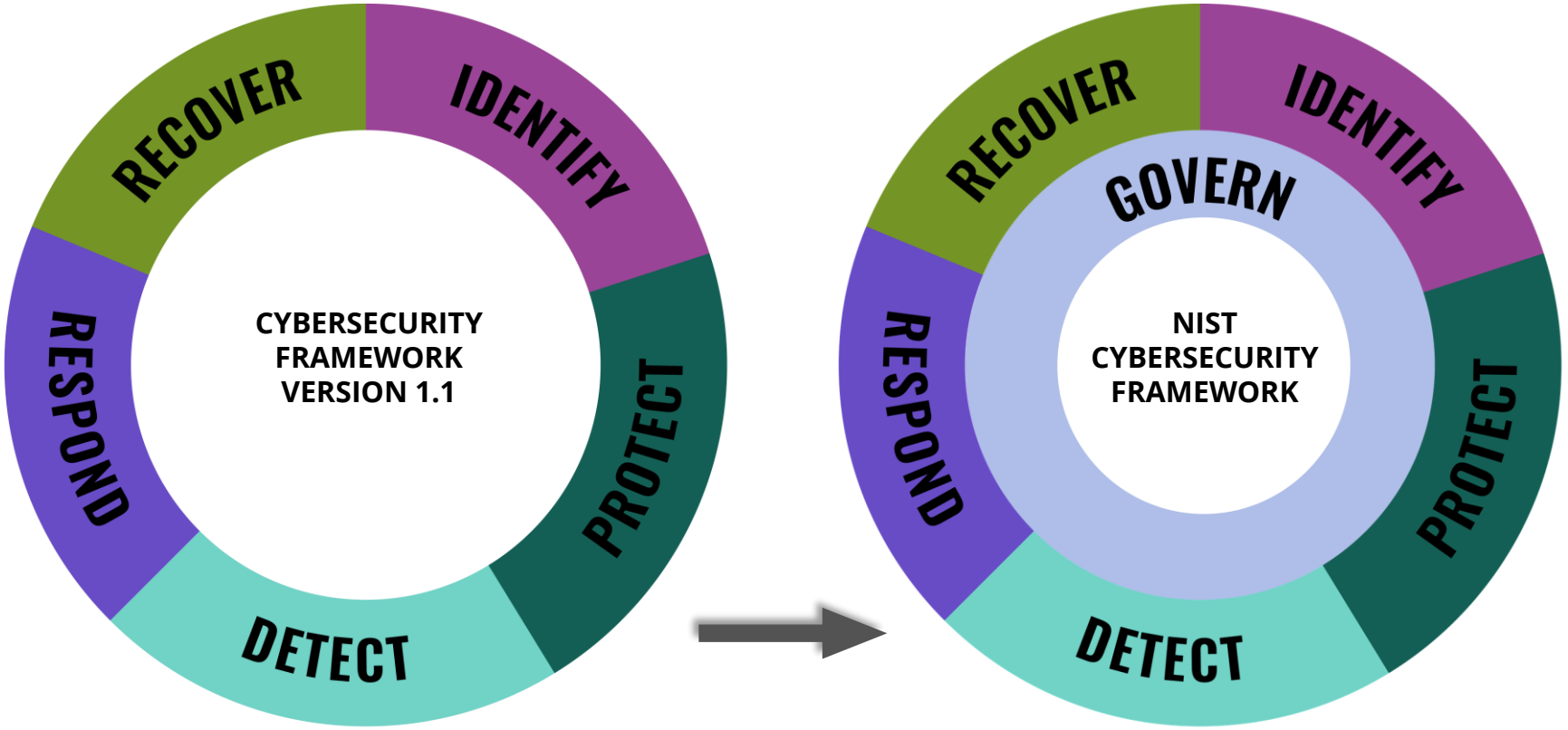
https://www.openkritis.de/eu/eu-nis-2-germany.html

Non-Compliance penalties

- Non-monetary remedies
- Fines
- Criminal sanctions

NIST CSF 2.0 – CORE FUNCTIONS AND ENHANCEMENTS

- New core function: Govern
- Focus on leadership, policy, and risk management
- Streamlined approach and clearer guidelines
- User-friendly resources: Quick Start Guides, searchable catalog
- Improved alignment with global standards



THE DRIVERS BEHIND THE CHANGE

Evolving Cybersecurity Landscape

With the increase in sophisticated cyber threats like ransomware and advanced persistent threats (APTs), there was a need to update the framework to better address these new forms of attacks.

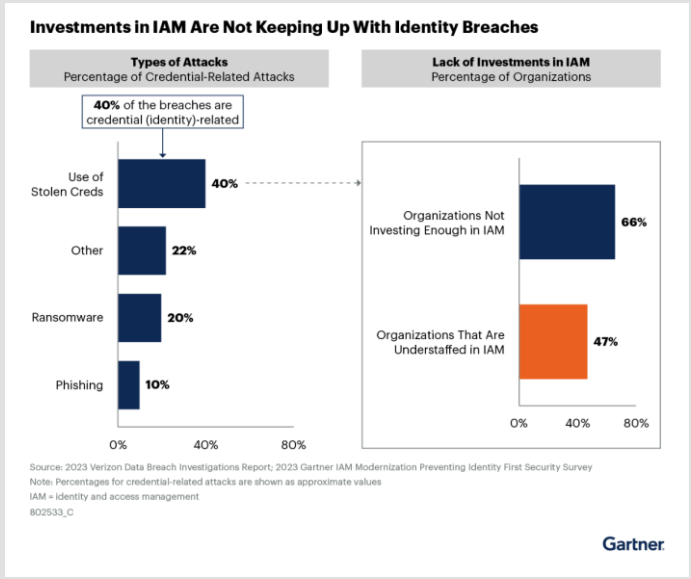
New Technological Challenges

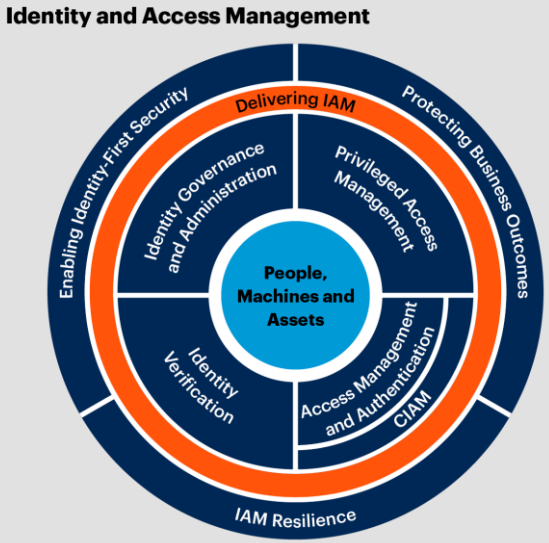
The rise of cloud computing and IoT devices has created new security vulnerabilities. NIST CSF 2.0 includes guidelines for securing cloud services and managing IoT device risks.

Continuous Improvement

Incorporating feedback from organisations that have used the original CSF, the new version emphasises iterative improvement and the importance of integrating cybersecurity with business processes.

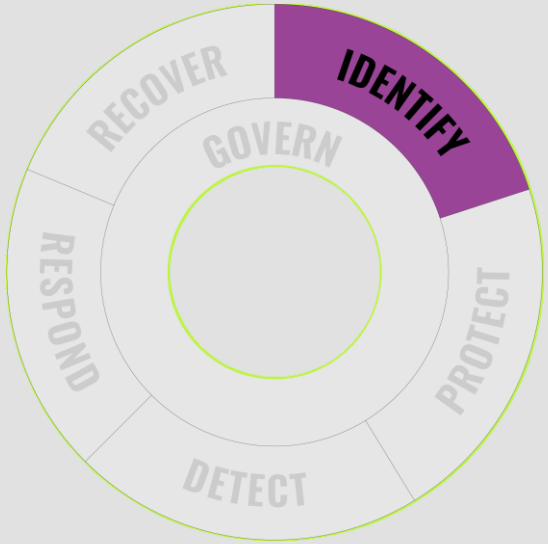
IDENTITY & ACCESS MANAGEMENT – WHY SHOULD THIS BE THE FOCUS ?





IDENTIFY

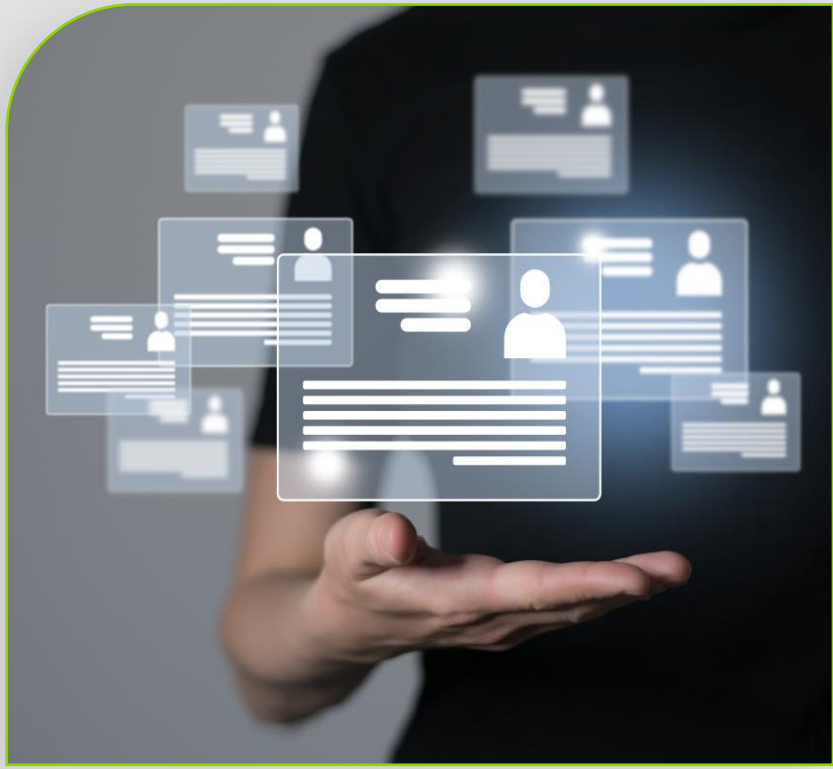
IAM and the Identify Function



01 | **Role of IGA in asset and identity management**. Identity Governance and Administration (IGA) helps organisations identify and manage digital assets and identities across their applications.

02 | **Creating and managing digital identities**. IGA tools enable the creation and management of digital identities, ensuring that only authorised individuals have access to specific resources.

03 | **Establishing a comprehensive inventory of digital assets.** This function is crucial for maintaining a comprehensive inventory of assets and identities, which is essential for the 'Identify' function of NIST CSF 2.0.



PROTECT

IAM and the Protect Function

01 | **PAM for securing privileged accounts**. PAM solutions enforce strict controls over privileged accounts, ensuring they are only accessible by authorised individuals. They include capabilities such as password vaulting, session recording, and monitoring of privileged activities.

02 | **AM for controlling user access**. AM solutions manage user access through authentication and authorisation mechanisms. This includes defining and enforcing access policies, managing user roles and permissions, and ensuring secure login processes.

03 | **Implementing MFA and SSO for enhanced security.** MFA adds an extra layer of security by requiring users to provide multiple forms of verification before accessing systems. SSO simplifies access management by allowing users to log in once and gain access to multiple applications.

DETECT

IAM and the Detect Function

01 **Monitoring and Analyzing Access Patterns.** IAM solutions continuously monitor access activities and log user actions. By analysing these access patterns, IAM tools can identify unusual behavior that may indicate a security threat.

02 **Detecting Anomalies and Unauthorized Access**. Advanced IAM solutions use machine learning and behavior analytics to detect anomalies and unauthorised access attempts. They compare current user activities against historical data to identify deviations from normal behaviour.

03 **Real-Time Alerts and Incident Response.** When an anomaly or unauthorised access is detected, IAM systems generate real-time alerts to notify security teams. This allows for immediate investigation and response to potential threats.

RESPOND

IAM and the Respond Function

01 **Incident Response Planning.** IAM solutions help organisations develop and implement incident response plans. IAM tools ensure that these plans are integrated with access management policies to facilitate swift and coordinated responses.

02 **Role-Based Access Control Adjustments.** During a security incident, it may be necessary to adjust access controls quickly to contain the breach. IAM systems allow for dynamic adjustments to role-based access controls, ensuring that access can be restricted or expanded as needed.

03 **Rapid Containment of Security Breaches.** IAM solutions enable rapid containment of security breaches by automatically blocking or restricting access based on predefined rules. This minimises the potential damage and prevents the spread of the breach.

RECOVER

IAM and the Recover Function

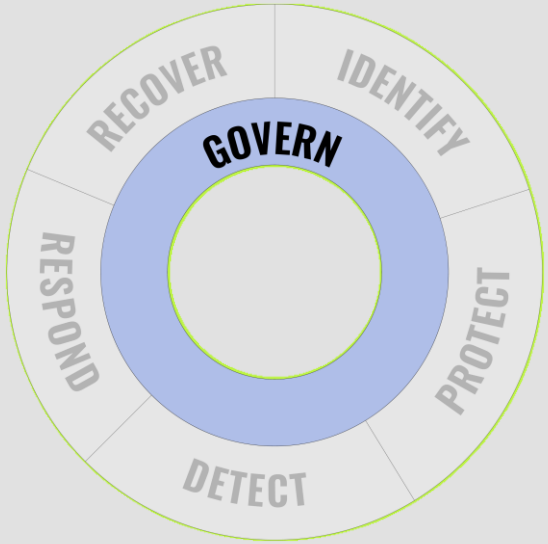
01 **Restoring Access Rights and Privileges.** After a security incident, IAM solutions facilitate the secure restoration of access rights and privileges. This involves verifying the identity of users and ensuring that they are granted the appropriate level of access based on their roles.

02 **Ensuring Continuity of Operations.** IAM solutions help ensure continuity of operations by maintaining secure access to critical systems and data during and after a security incident. This includes implementing backup authentication mechanisms and providing secure temporary access to essential resources.

03 **Post-incident Reviews and Improvements.** IAM solutions facilitate post-incident reviews by providing detailed logs and reports of access activities. Based on these insights, organisations can implement improvements to their IAM policies and procedures, enhancing their overall security posture and preventing future incidents.

GOVERN

IAM and the Govern Function



01 **Establishing Cybersecurity Governance Policies.** IAM solutions help establish robust governance policies by defining clear roles and responsibilities for managing digital identities and access. These policies ensure that all aspects of identity and access management are governed by consistent and comprehensive rules.

02 **Integrating IAM with Risk Management Strategies.** IAM integrates with broader risk management strategies by providing a comprehensive view of identity and access risks. This integration allows organizations to align their IAM practices with their overall risk management objectives.

03 **Ensuring Leadership Commitment and Oversight.** IAM solutions provide the necessary tools for leadership to monitor and enforce compliance with cybersecurity policies. Dashboards and reports offer visibility into identity and access activities, enabling leaders to make informed decisions and ensure that governance policies are effectively implemented and adhered to across the organisation.

NEXT STEPS / CALL TO ACTION

01

Where are you on your IAM journey ?

- An assessment of what you have already
- Where do you want to get to ?
- What are the priorities ?
- Where are the gaps ?

02

Create a plan

- Overall Strategic plan – what does the target look like ?
- Broken down into small, bite-sized chunks. Prioritise biggest risk gaps and quick wins
- Costed and include Return on Investment (ROI) metrics

03

It’s not just about the technology !

- Having the right people and sponsorship to deliver change is as important
- Involve experts who know the journey and can guide you
- There is no finish line, partner with a company who can evolve with you and provide the expertise and resourcing you need to remain protected

Thank you !

If you wish to learn more or talk to us at Intragen you can reach me:

Paul.Cameron@intragen.com
+44(0) 7376 22 1986

Or get started with one of our pre-packaged Maturity Assessments to start your journey to NIS2 compliance with IAM

https://www.intragen.com/maturity-assessment