What the SOC!?
Clarifying the Audit Certificate Chain and Shared Responsibility

Jay Thoden van Velzen
Strategic Advisor to the CSO, SAP

What if SAP Software Stopped Working Today?

Stage 1

Electronic Transactions Stop

- Cash-only required to buy anything – ATMs soon run out or do not work
- Shops run out of perishable goods, black markets emerge
- Hungry citizens do what they must

Stage 2

Supply Chains Break Down

- Gas stations run out, shops and facilities no longer are replenished
- Manufacturing shuts down
- Energy generation and distribution stops
- Transportation stops

Stage 3

Civil Unrest and Disorder

- Social order breaks down without authorities having an ability to respond
- Lines of communication break
- Command structures rendered ineffective
- Total Societal Collapse

Existential Cyber Risks

Regulatory Audit Failure

- Failed 3rd party audit for regulatory compliance (ISO/SOC, C5/KRITIS, FedRAMP, HIPAA, etc.)

Cause

- Organizational indiscipline
- Impossible policy requirements

Mitigation

- Governance and Accountability

Data Extortion or Destruction

- Loss or exposure of individual customer data
- Mass extraction or destruction of customer data

Cause

- Leaked credentials/phishing
- “Ransomware”

Mitigation

- Secrets Mgt, CSPM, IAM, MFA

Nation State Attack or Action

- Intelligence/Cyber Espionage
- Disruptive/Destructive Attacks

Cause

- Advanced Persistent Threats
- Zero Days, Endless Resources

Mitigation

- Resilient security capabilities

Security Risks Driving Priorities

High Level Risk Categories to Focus on the Most Critical as a Cloud Service Provider

Common Sources of Security Breaches

- Cloud infrastructure misconfigurations, known vulnerabilities and leaked credentials are the most common sources of cloud security breaches
- Compliance with security policies and hardening procedures, enterprise vulnerability management and managing secrets protects SAP against these threats

Risks Affecting SAP and Employees

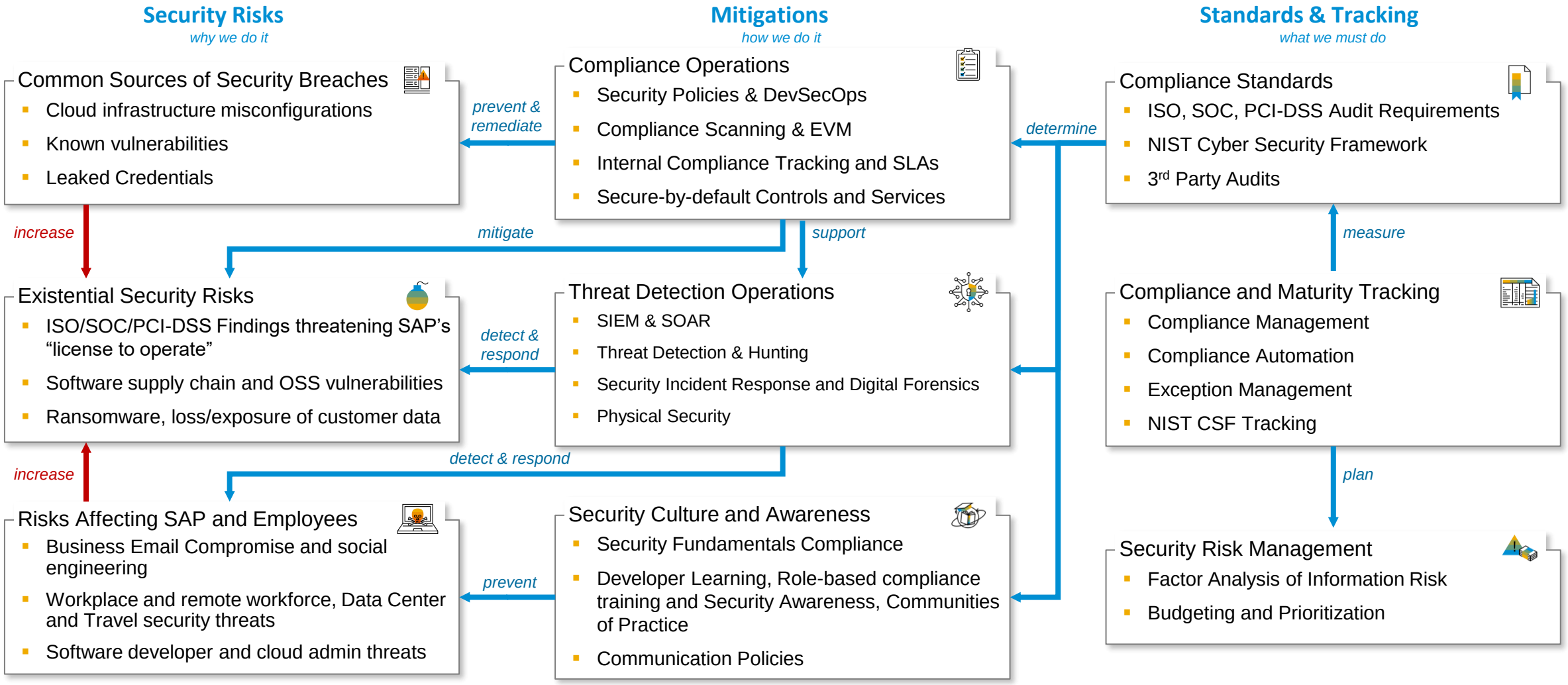
- Threats against employees remain relevant, such as social engineering, loss or theft of equipment, or physical threats against employees or facilities
- Cloud admins and those with access to source code and CI/CD pipelines at particularly risk
- A vigilant workforce that is prepared for their security role in the organization and appropriate controls protects SAP against such threats

Existential Security Risks

- Failure to meet audit certification and regulatory compliance, or a security breach exposing or destroying customer data would be detrimental to SAP’s strategic goals and the company’s future
- Brand reputational loss would increase if proven to having failed our own security policy standards and commitments
- Best-in-class security and compliance operations mitigates against these security risks

Best-in-Class Security & Compliance Operations Protect SAP

Compliance contributes greatly to reducing security risks



NIST CSF Framework Core Functions

NIST CSF Control Coverage

Identify	Protect	Detect	Respond	Recover
▪ Asset Management ▪ Business Environment ▪ Governance ▪ Risk Assessment ▪ Risk Management Strategy ▪ Supply Chain Risk Management	▪ Identity Management and Access Control ▪ Awareness and Training ▪ Data Security ▪ Information Protection Processes and Procedures ▪ Maintenance ▪ Protective Technology	▪ Anomalies and Events ▪ Security Continuous Monitoring ▪ Detection Processes	▪ Response Planning ▪ Communications ▪ Analysis ▪ Mitigation ▪ Improvements	▪ Recovery Planning ▪ Improvements ▪ Communications
Asset and Risk Management	Preventive Measures	Scans and Analysis	Response and Remediation	Resiliency and Recovery

- A common cybersecurity framework maintained by the US govt. National Institute of Standards and Technology
- Current revision 1.1 – a 2.0 draft is available for feedback

- Defines a comprehensive set of core controls and multiple tiers
- Tiers describe “an increasing degree of rigor and sophistication in cybersecurity risk management practices”

- Good guideline to build security programs on, and what functions and processes need to exist
- Familiar to auditors
- Self-select the ones you will commit to doing

NIST CSF Framework Implementation Tiers

Indicating Maturity

Source: NIST CSF v.1.1

Tier 1: Partial

- Risk Management Process
  - Organizational security risk management (RM) practices not formalized, risk managed in an ad hoc and reactive manner. Prioritization of activities not directly informed by organizational risk objectives, threat environment, or business/mission requirements
- Integrated Risk Management Program
  - Limited awareness of security risk at the org level. RM on an irregular, case-by-case basis. No processes that enable security information to be shared within the organization
- External Participation
  - Org does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information from other entities, nor does it share information. Org generally unaware of the cyber supply chain risks of the products and services it provides and that it uses

Tier 2: Risk Informed

- Risk Management Process
  - RM practices are approved by mgt but may not be established as org-wide policy. Prioritization of security activities and needs is directly informed by org risk objectives, threat environment, or business/mission requirements
- Integrated Risk Management Program
  - Awareness of security risk at org level, but an org-wide approach to RM has not been established. Security info is shared within the org on an informal basis. Consideration of security in org objectives and programs may occur at some but not all levels. Risk assessment occurs, but is not typically repeatable
- External Participation
  - Org understands its role in the ecosystem wrt either its own dependencies or dependents, but not both. Org collaborates with and receives some info from other entities and generates some of its own, but may not share with others. Org is aware of the supply chain risks, but does not act consistently or formally upon those risks

Tier 3: Repeatable

- Risk Management Process
  - Org's RM practices are formally approved and expressed as policy. Org security practices are regularly updated based on the application of RM to changes in business/mission requirements and a changing threat and technology landscape
- Integrated Risk Management Program
  - Org-wide approach to RM is defined, implemented as intended, and reviewed. Consistent methods in place to respond effectively to changes. Personnel possess the knowledge and skills to perform their roles and responsibilities. The org consistently and accurately monitors security risk. Sr. security and non-security execs communicate regularly regarding security risk and ensure consideration of security through all lines of operation in the org
- External Participation
  - Org understands its role in the ecosystem, contributes to the community's broader understanding of risks, and collaborates with and receives info from other entities complementing internal info, and shares info with others. Org is aware of supply chain risks and acts formally upon those risks, incl. written agreements of baseline requirements, governance structures, and policy implementation and mor

4. Adaptive

- Risk Management Process
  - Org adapts its security practices based on previous and current security activities, incl. lessons learned and predictive indicators. Through continuous improvement incorporating advanced security technologies and practices, the org actively adapts to changing landscapes and responds in a timely and effective manner to evolving, sophisticated threats
- Integrated Risk Management Program
  - Org-wide approach to RM that uses risk-informed policies, processes, and procedures to address potential security events. Relationship between security risk and org objectives is clearly understood. Sr. execs monitor security risk like they do financial- and other org risks. Budget is based on RM. BUs implement RM in the context of org risk tolerances. RM is part of the org culture and evolves from continuous awareness. Org can quickly and efficiently account for changes to business objectives
- External Participation
  - Org understands its role in the ecosystem and contributes to the community. It receives, generates, and reviews prioritized info that informs continuous risk analysis as landscapes evolve. Org shares that info internally and externally with other collaborators. The organization uses (near) real-time info to understand and act upon supply chain risks, and communicates proactively

Cyber Resiliency

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.

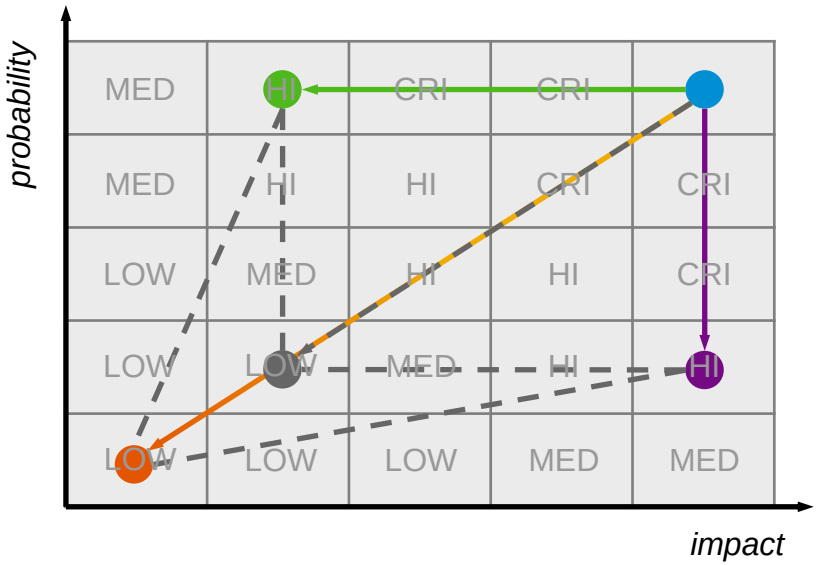
NIST 800-171r2

Recover

- Recovery measures reduce the **impact** of security incidents

Detect

- Detective measures allow for greater visibility in security compliance posture and threats



Protect

- Protective measures reduce the **probability** of security incidents

Respond

- Response capabilities reduce time to action whether in compliance findings or active threats

Cyber Resiliency

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.

NIST 800-171r2

Tools

- Commercial and Open Source security technology
- Automation

Processes

- Operationalization of tools
- Runbooks/playbooks
- Organizational accountability

People

- Comfortable with processes
- Collaborative, enabling
- Learn from mistakes

From NIST/ISO Control to Policy and Audit

NIST/ISO Control

What you must do

- The standard control list or framework states high-level requirements
- They don't tell you how to achieve them

Policy Definition

How you are going to do it

- Defines the specific policy controls for the organization
- Must be able to provide evidence that the policy is followed

3rd Party Audit

Prove that you are doing it

- Third party auditors will base their assessment on *your policies* and proof you follow them
  - ISO: are you doing it now?
  - SOC: have you been doing this the last six months?

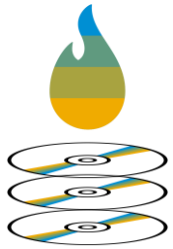
So it is important you set policies your organization can achieve – especially in emergency circumstances!

Beware of Idealistic Policy Definitions Without Resilience

Example for Illustration – *Don't get too specific or fail to consider emergency scenarios!*

Destruction of Physical Media

- Scenario
  - A set of hard drives are set to be destroyed
  - Normal supplier has no capacity, the next option is 300 miles away
  - No salaried employee able to travel
  - Team takes the media to the parking lot and records the entire process on their cellphone



Policy A

- Lock media securely prior to destruction
- Video record the entire process from secure storage to media destruction

Audit Outcome

Policy B

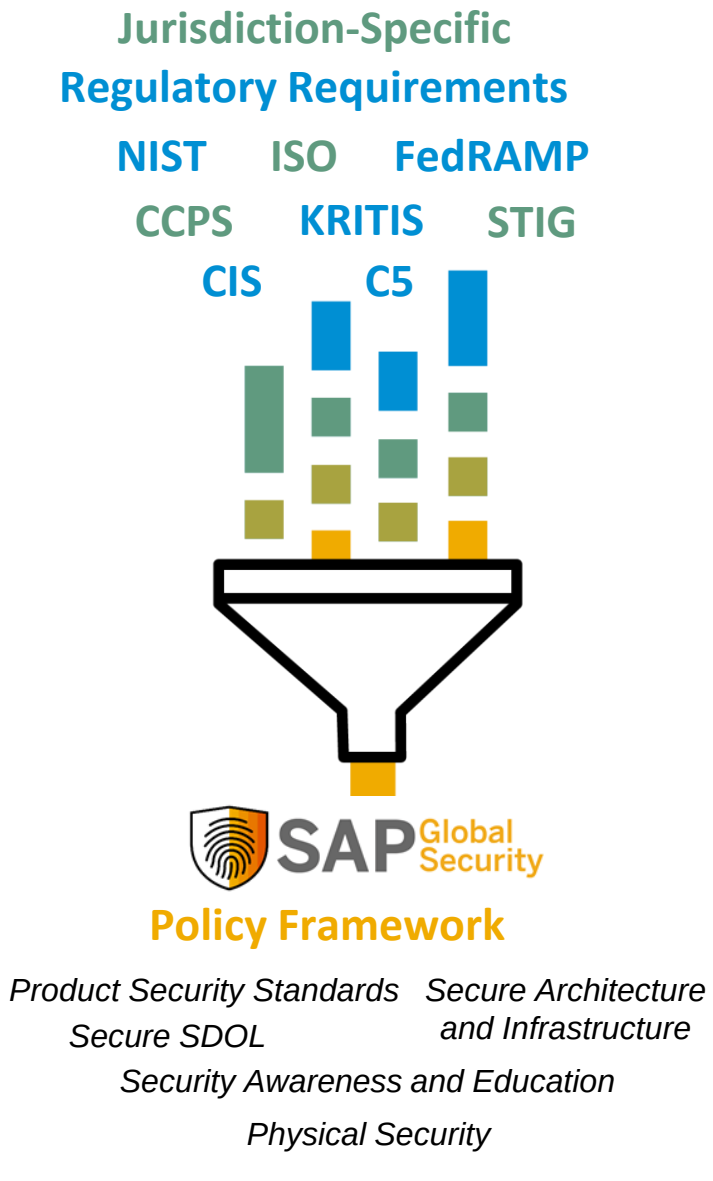
- Lock media securely prior to destruction
- Transport media to destruction site in a locked box
- Salaried employee must witness an approved 3rd party provider shred the media
- Employee must sign off that media were destroyed according to policy

Audit Outcome

Policy Making at SAP

Policy-Once, Audit-Many

- SAP and its customers operate in many different jurisdictions, with different audit regimes
- SAP abstracts policies from all these requirements to ensure teams only have to follow one set of guidelines



Policy Coverage

- Overall policy coverage determined by NIST CSF controls (broad coverage)
- SAP Cloud Solutions primarily covered by product security, secure development and operations lifecycle, and architecture and infrastructure policies

SAP Cloud Landscapes and NIST CSF Framework Core Functions

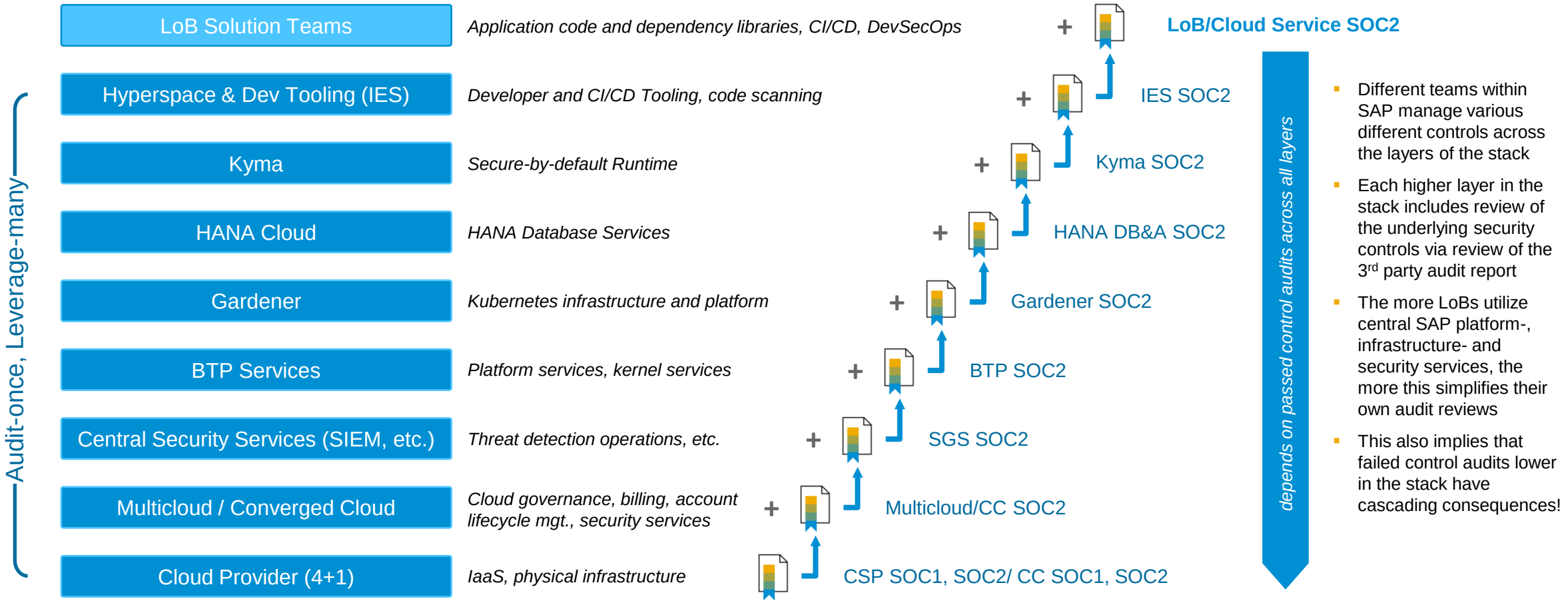
NIST CSF Controls Implemented and Operational

Identify	Protect	Detect	Respond	Recover
▪ Asset Management ▪ Business Environment ▪ Governance ▪ Risk Assessment ▪ Risk Management Strategy ▪ Supply Chain Risk Management	▪ Identity Management and Access Control ▪ Awareness and Training ▪ Data Security ▪ Information Protection Processes and Procedures ▪ Maintenance ▪ Protective Technology	▪ Anomalies and Events ▪ Security Continuous Monitoring ▪ Detection Processes	▪ Response Planning ▪ Communications ▪ Analysis ▪ Mitigation ▪ Improvements	▪ Recovery Planning ▪ Improvements ▪ Communications
Asset and Risk Management	**Preventive Measures**	**Scans and Analysis**	**Response and Remediation**	**Resiliency and Recovery**
▪ CCIR/SISM, MCDB and metadata tagging ▪ Cloud accounts by policy in SAP cloud organizations ▪ Central scans and asset discovery ▪ Threat intelligence ▪ Risk assessment and FAIR quantitative risk management ▪ TPRM and Office of OSS Mgt ▪ Internal and 3rd party audits	▪ Cloud guardrails and secure resource orchestration, incl. Golden Images ▪ IAM, MFA and Cloud Infrastructure Entitlement Mgt (CIEM) ▪ Mandatory Security Fundamentals, DevLearning, 3rd party training, events ▪ Data Privacy and Protection ▪ Security policies, processes and validation (DevSecOps) ▪ CI/CD build checks	▪ Continuous CSPM and CNAPP scans, cloud audit logs ▪ Host and container runtime detection, vulnerability scans ▪ Network security, incl. IDS/IPS, WAF, DNS ▪ SIEM ingestion, data enrichment, automation, distribution and reporting ▪ Threat detection and hunt	▪ Cyber Fusion Center, incl. SIEM, SOAR, DFIR and SOC ▪ LoB security response teams ▪ Incident communication processes ▪ Security and compliance reporting, dashboarding, SLA tracking, audit findings mgt. ▪ BISO Council, Security Execution, Office Hours ▪ Continuous improvement	▪ Cyber resiliency processes, incl. primary and secondary back-ups, CI/CD, anti-ransomware ▪ Product security response and patch management ▪ Post-incident RCA and continuous improvement ▪ Trust Office, Cyber Legal and Outside Communications

Audit Certification Chains, Operational Efficiency and Shared Fate

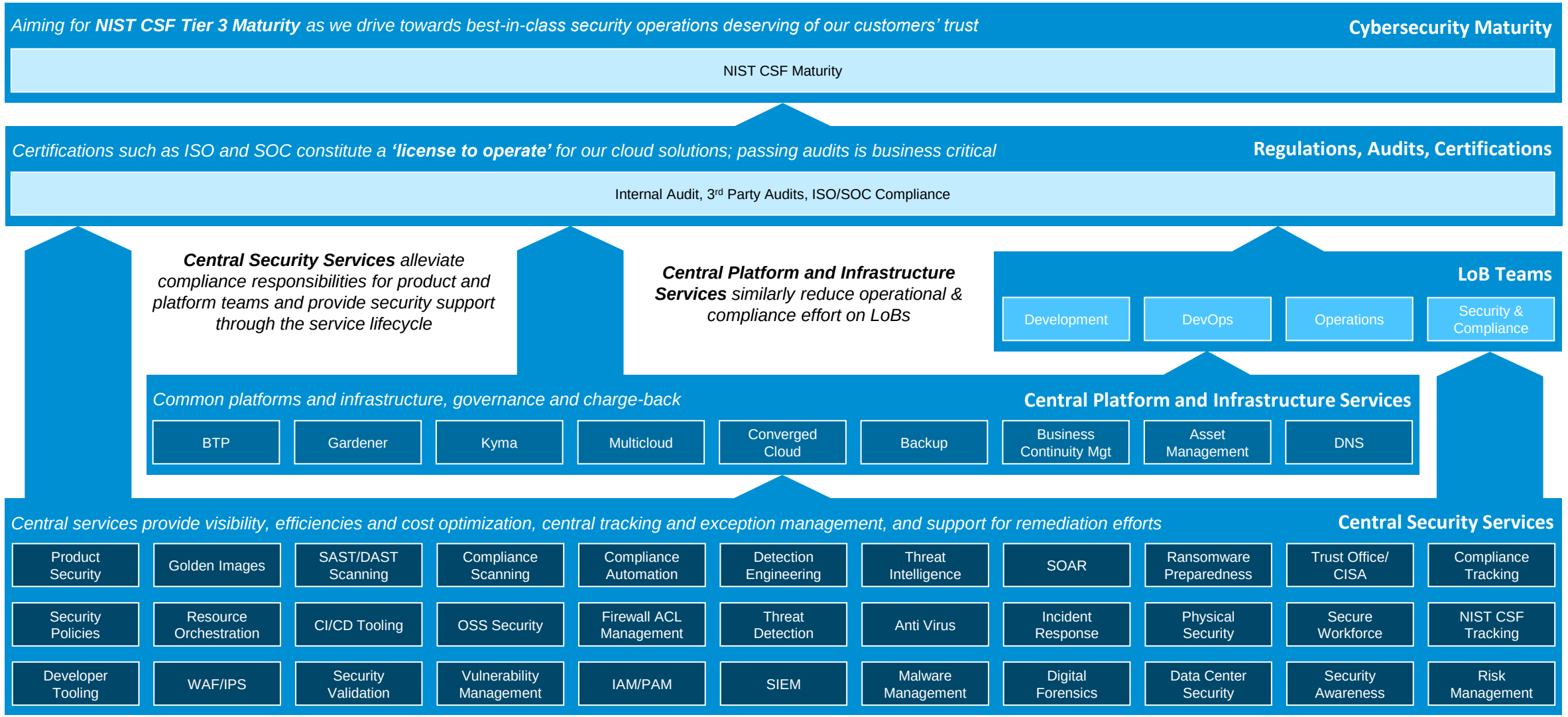
We Are All In This Together – Example: SOC2 Certification

- Central services used by LoB teams imply more controls are handled by central teams, increasing operational efficiency in audits – as long as the central teams providing them meet their own control audit requirements



- Different teams within SAP manage various different controls across the layers of the stack
- Each higher layer in the stack includes review of the underlying security controls via review of the 3rd party audit report
- The more LoBs utilize central SAP platform-, infrastructure- and security services, the more this simplifies their own audit reviews
- This also implies that failed control audits lower in the stack have cascading consequences!

Shared Fate in Security Compliance and Cybersecurity Maturity

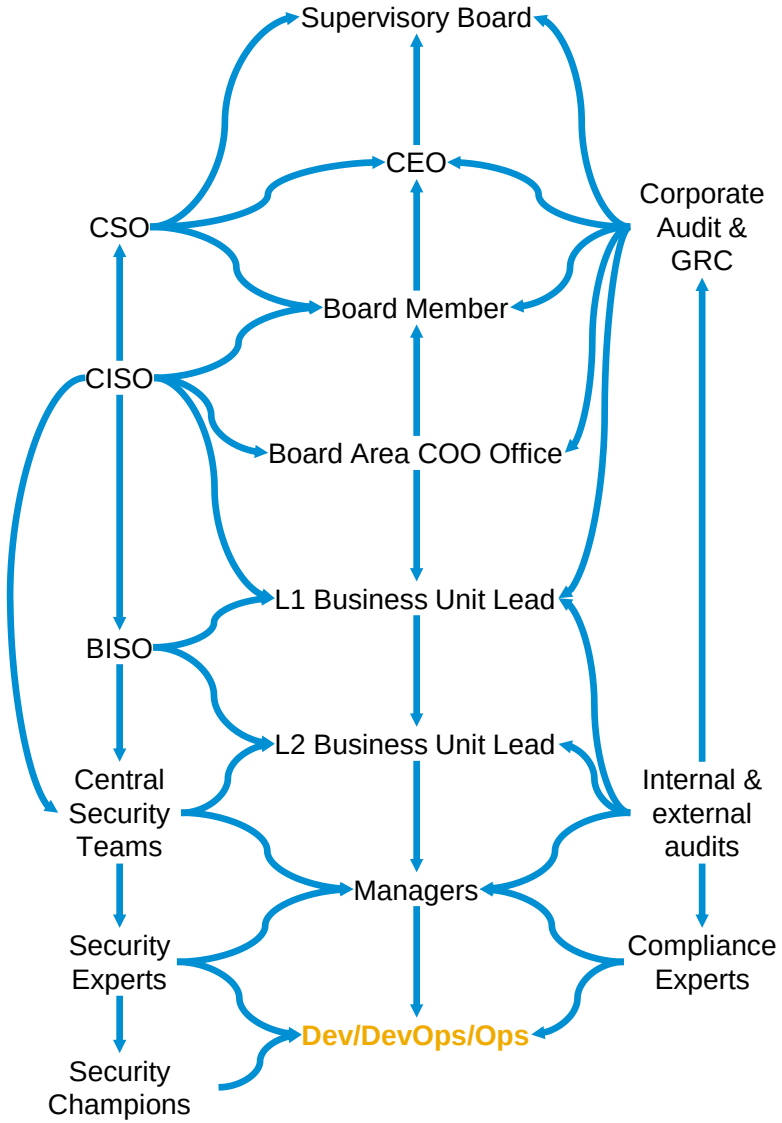


Accountability Throughout the Organizational Hierarchy

Making Security Matter

Reporting and SLA Tracking

- Experience shows policies are not followed unless verified
- Central security and compliance scans alone do not make an organization move
- Multi-level reporting and SLA tracking
- Multiple layers of accountability established throughout the organizational hierarchy to ensure alerts are followed up on
- Regular EB/SVB, L1, Board Area Delegate, BISO Council, Office Hours Meetings
- *Quis custodiet ipsos custodes?* Corporate Audit



Cut Through Competing Priorities

- Security competes with many different priorities – both within technical teams as higher up the organizational hierarchy
- Developers and DevOps Engineers don't set priorities – managers do, VPs do
- Security and Audit & Compliance support is needed to ensure priorities are understood

Cyber Resiliency Through Compliance

Compliance is not Security?

OK. But…

Compliance is how Security gets funded

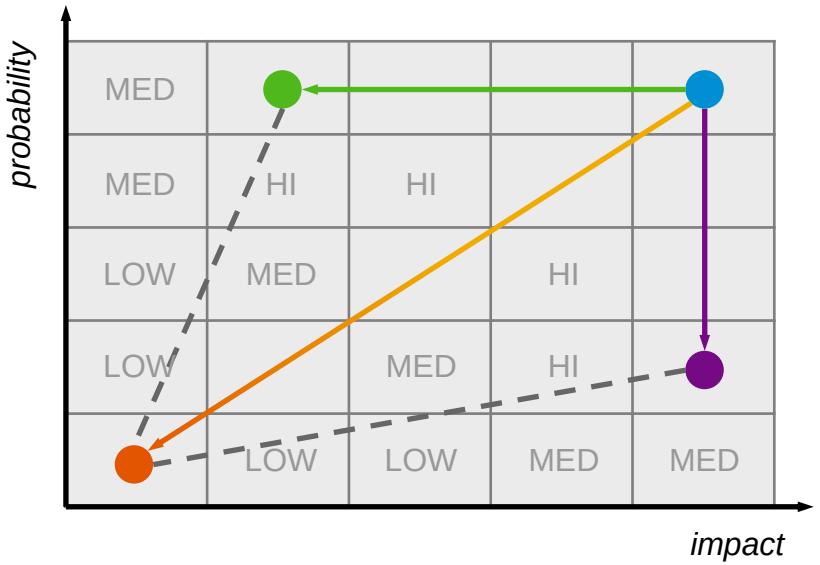
It is up to us in security roles to ensure we get the best outcomes out of available budget and resources

Recover

- Recovery measures reduce the **impact** of security incidents

Detect

- Detective measures allow for greater visibility in security compliance posture and threats



Protect

- Protective measures reduce the **probability** of security incidents

Respond

- Response capabilities reduce time to action whether in compliance findings or active threats

SAP NOW

Future Proof Your Business

Save The Date

Date: August 8, 2023

Venue: The Hyatt Regency, Sydney

More details coming soon

Thank you.

Contact information:

Jay Thoden van Velzen

jay.thoden.van.velzen@sap.com
@jaythvv@infosec.exchange
https://www.linkedin.com/in/jay-thoden-van-velzen/

Keeping SAP Customers Secure Around the Globe
Taking a Risk-Based Approach to Protect Customer Data by Implementing the NIST Cybersecurity Framework

- Vanessa Barber (SAP SE), Hedayatollah Hosseini (SAP SE), and Dr. Peter Westphal (Ernst & Young), sap.com, 2023

THE BEST RUN SAP