

# SIAM challenges

Challenges, risks, considerations

*Extracted from the ITSM Zone SIAM  
course*

# Challenge areas

- Building a business case
- Level of control and ownership
- Commercial challenges, including legacy contracts
- Cultural fit, collaboration and cooperation
- Measuring success
- Trust and eliminating micro-management
- Security

# Business case

- Who is affected? – The customer
- Without business case, the transformation to SIAM might never begin
- The cost of the SIAM transformation needs to be factored in and compared to any potential cost savings

# Business case risks

- The customer organization might not approve the transition to SIAM
- The customer organization approves the business case, but does not allocate enough resources and investment
- The customer organization has no clear vision of the expected benefits
- The success of the program cannot be measured
- The costs are underestimated

# Business case – risks mitigation

- Allocating skilled resources to build the business case, possibly using external support
- Linking the SIAM strategy to the overall customer strategy, and then identifying and addressing each SIAM driver
- Adding as much detail as possible and documenting expected benefits, as well as continual refinement

# Business case – risks mitigation

- Include a proposed SIAM structure and model
- Identify any current contracts that are inefficient or wasting money
- Look for industry data and benchmarks that can help to show the benefits of SIAM in other, similar organizations

# Challenges - Level of control and ownership

- Who is affected? – The customer, as it makes decisions about the SIAM structure and model
- The customer needs to make decisions and give clear guidance so that the service integrator and service providers understand what they need to do

# Risks- Level of control and ownership

- Lack of clarity about the level of control and ownership
- One organization saw little benefits from SIAM because it used its own staff to shadow the service integrator staff
- Referred to as 'man-marking'



# Risks- Level of control and ownership

- The service integrator being unable to perform its role, because the customer hasn't delegated any tasks
- Data is too tightly controlled, so the service integrator and the service providers don't have access to data they need to fulfill their role
- Ownership of data isn't defined, so the customer loses control of its data
- Too little control:
  - If the customer organization delegates everything, the service integrator might not have enough strategic direction to be effective
  - Customer at risk of data breach

# Commercial challenges

- All parties need to feel they are getting a fair deal
- Legacy contracts refer to the contracts that a customer organization has already signed
- These might not be fit for purpose in the new SIAM model or might expire

# Commercial challenges

- Who is affected? - All parties
- If a service provider feels it is being treated unfairly, or has been transitioned into a SIAM model under inappropriate contract, it will be less willing to collaborate and communicate
- This will make the service integrator's role harder and will affect the value that can be delivered

# Risks - Commercial challenges

- Service providers who feel their contract is unfair
- Poorly defined service boundaries
- A lack of service integrator empowerment
- Service providers might impose their own contracts – the service integrator need to adapt to this

# Risks – Commercial – Legacy contracts

- Increased costs: these could include paying for an extension to a contract that is due to, or paying to exit a contract early
- A gap in service, where legacy contract has expired before the SIAM model is established
- Increased workload for the service integrator trying to integrate the legacy contracts into the SIAM model

# Challenges - Security

- Who is affected? – All layers
- Each layer will have roles and responsibilities that support the security of the overall model
- Security considerations need to be addressed during Plan and Build
- If they are not designed during the early parts of the roadmap, they will have to be addressed retrospectively

# Risks - Security

- Commercially sensitive data might be shared inappropriately between service providers, and security tasks might be duplicated or not carried out at all

# Challenge – Measuring success

- The customer organization will expect to achieve business value from adopting to SIAM
- If it cannot measure its SIAM model, it will not be able to demonstrate business value
- The service integrator's role will be more difficult without effective reporting framework, and it won't be able to indentify improvements
- Measures should be defined during Plan and Build



# Risks – measuring success

- No effective end to end reporting framework
- Measurements that do not align with or provide evidence to support the business case for SIAM
- Not measuring the right things or measuring too much information, or not measuring enough

# Mitigation – measuring success

- Effective performance management and reporting framework
- Identify during Plan and Build what will be measured, when, how, by whom and why.

# Challenge – Trust and micro-management

- SIAM is built on communication and good relationships
- Lack of trust can manifest in two areas
  - Lack of trust between the customer and the service integrator
  - Lack of trust between the service integrator and the service providers

This can lead to micro-management and increased costs related to unnecessary checks

# Challenge- Trust and micro-management

- Affects all organisations
- Identified often during Run and Improve stage

# Mitigation – lack of trust and micro-management

- If clear roles and responsibilities are developed during Plan and Build, lack of trust can be identified more easily
- A phased implementation using structural elements like process forums and working groups will build relationships and trust
- Micro-management should be managed as an opportunity for improvement

# Challenge - Culture

- Affects all parties
- The customer needs to lead by example
- Culture needs to be addressed during Plan and Build, or issues will be felt during Implement and Run and Improve

# Risks - Culture

- Service providers not interacting with each other, or with end to end processes and procedures
- Service targets not being met and benefits not delivered
- The service integrator being unable to fulfil its role due to poor working relationship with service providers

# Challenge - DevOps

- Can cause issues in a SIAM environment
- The Service Integrator role can be seen as unnecessary interference
- A SIAM model that includes segregation of duties and service elements split between multiple service providers can be in conflict with DevOps thinking



# Challenges – Integrated processes

- Service providers don't integrate their processes or share process details
- Gaps between process activities
- Time-consuming and manual reporting
- Poor relationship between service providers - blame culture

# Challenges – Integrated processes

- Complexity – the more complex a process is, the more challenging it can be to manage
- SIAM complexity
  - Processes span SIAM layers
  - Increased number of organisations involved
  - Processes need to be integrated
  - Process interactions can take place between organizations

# Data and information considerations

- Who owns the data? Does the customer organization have access to it if the relationship with an external organization ends?
- Who owns the IP for artefacts, e.g. Knowledge articles?
- Is data and information consistent between toolsets?
- How is access to shared data, information and tools controlled, and how are security standards maintained?
- How will any compliance and assurance requirements be managed?

# Considerations - Improvement

- Who is responsible for process improvement?
- Each party is accountable for improving their own processes, and contributing to end to end process improvement