2nd Annual Workshop on Cyber Security in HPC (S-HPC'23).

Invited Talk:

Information Security Controls Prioritisation: SABSA for HPC.

Nicolás Erdödy - Open Parallel Ltd. / Multicore World (Presenter).
Duncan Hall – IEEE Computer Society, IEEE Life Senior Member.

November 12th, 2023 - Denver, CO, USA.
In conjunction with the 35th International Conference for HPC, Networking, Storage and Analysis.

Disclaimer:

Duncan Hall

“Opinions expressed in this presentation are mine.”

“The opinions do not necessarily reflect the views of my employer, Manatū Aorere – New Zealand Ministry of Foreign Affairs and Trade, nor the New Zealand Government.”

About:


OpenParallel


2024
MulticoreWorldXI
11th Edition | 12 -16 February 2024 | Christchurch, New Zealand


ListentotheLand


WhakarongokiteWhenua


EURÓPAI UNIÓ
MAGYAR KÖZTÁRSASÁG
ÚTLEVÉL
NEW ZEALAND
PASSPORT
URUWHENUA
AOTEAROA
MERCOSUR
REPUBLICA ORIENTAL
DEL URUGUAY
PASAPORTE

Background - SKA (now SKAO).

ListentotheLand

Originally planned to process 157 Tb/sec –

(actual Exascale Computing).

Now…

- Square Km Array Observatory.
- Next-gen radio telescopes.
- Australia - South Africa.
- Big Science.
- Megaprojects.
- Truly global.
- Platforms.
- Vision vs. Reality - 15Tb/s
- “Like a startup”.
- 2011-2019

Considerations for the SDP Operating System

Document Number.....SDP Memo 063
Document Type.....MEMO
Revision.....01
Author.....N. Erdödy, R. O'Keefe
Release Date.....2018-08-31
Document Classification.....Unrestricted
Status.....Draft

Document No: 063
Revision: 01
Release Date: 2018-08-31

Unrestricted
Author: N. Erdödy
Page 1 of 56

Security for the SDP
Architecture Considerations

Document Number.....SDP Memo 064
Document Type.....MEMO
Revision.....01
Author.....N. Erdödy, R. O'Keefe
Release Date.....2018-08-31
Document Classification.....Unrestricted
Status.....Draft

Document No: 064
Revision: 01
Release Date: 2018-08-31

Unrestricted
Author: N. Erdödy
Page 1 of 37

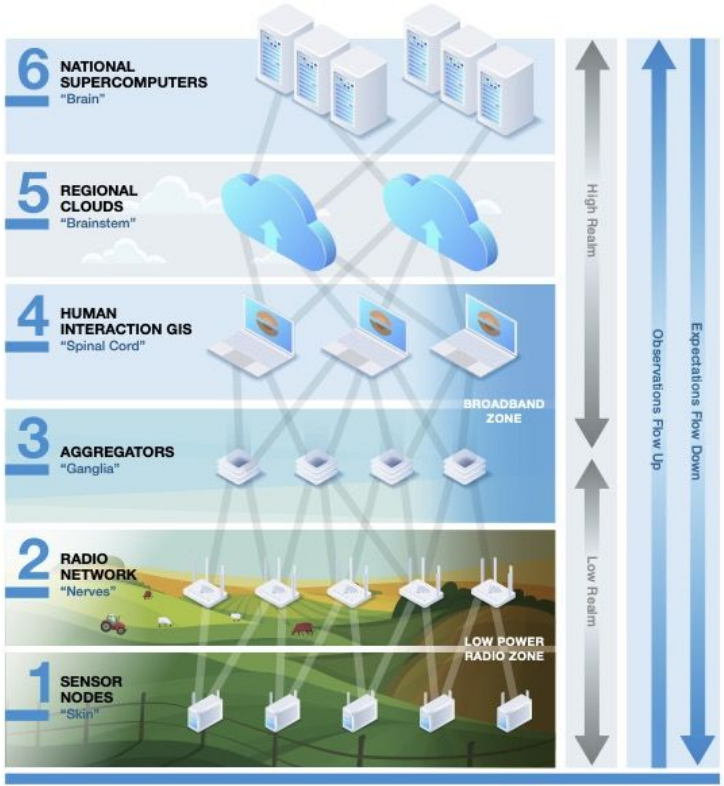
Available https://ska-sdp.org/publications/released-sdp-memos-1

OpenParallel

ListentotheLand

Agriculture Empowered by Supercomputing

Nation-Wide Digital Nervous System



OpenParallel

Outline:

- **Background: SKA; Listen to the Land.**
- **HPC: Speed above all; Special challenges.**
- **NIST SP 800-223: Complications; Questions; Some Answers.**
- **What is SABSA?**
- **SABSA in context: A linear programming construct.**
- **Summary: SABSA's benefits; A call to action.**

HPC – speed at the expense of all else?

- **2009 – 2012: SKA Program Development Office experiences** (SPDO) - Duncan Hall.

- **2017 - 2018: SKA - Meltdown and Spectre.** (Science Data Processor -SPD) - NE.

- **NIST's Computer Security Resource Center (CSRC).**

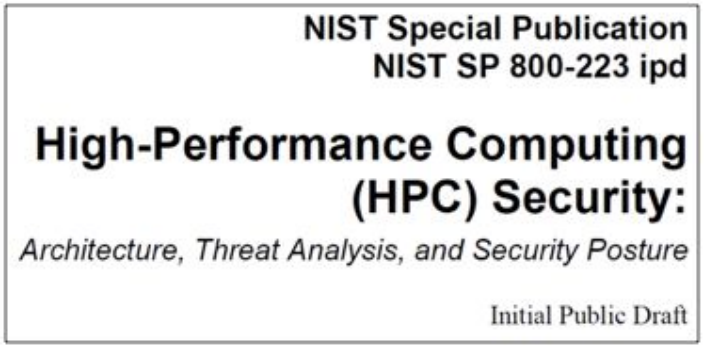
  To help the **"HPC community to create a HPC Risk Management Framework (RMF) it shall provide a comprehensive and reliable security guidance to identify, eliminate and minimize risks in the use, operation and management of HPC systems"**

HPC – special challenges

- **"Securing HPC systems is challenging due to their size; performance requirements; diverse and complex hardware, software, and applications; varying security requirements; and the nature of shared resources."**

- **"The security tools suitable for HPC are inadequate, and current standards and guidelines on HPC security best practices are lacking."**

- **"The continuous evolution of HPC systems makes the task of securing them even more difficult."**



NIST SP 800-223 Section 5. Conclusions, page 19.

Also watch:

“How HPC Can Avoid Sophisticated Security Breaches”

Dr. Albert Reuther, senior staff member in the MIT Lincoln Laboratory.
Co-author of NIST 800-223.

HPC Tech Talk (Dell) - 7 October 2023.
https://www.youtube.com/watch?v=_MsuQDSVu20 (25’)

Outline:

- Background: SKA; Listen to the Land.
- HPC: Speed above all; Special challenges.
- NIST SP 800-223: Complications; Questions; Some Answers.
- What is SABSA?
- SABSA in context: A linear programming construct.
- Summary: SABSA's benefits; A call to action.

NIST SP 800-223 reference architecture for HPC:

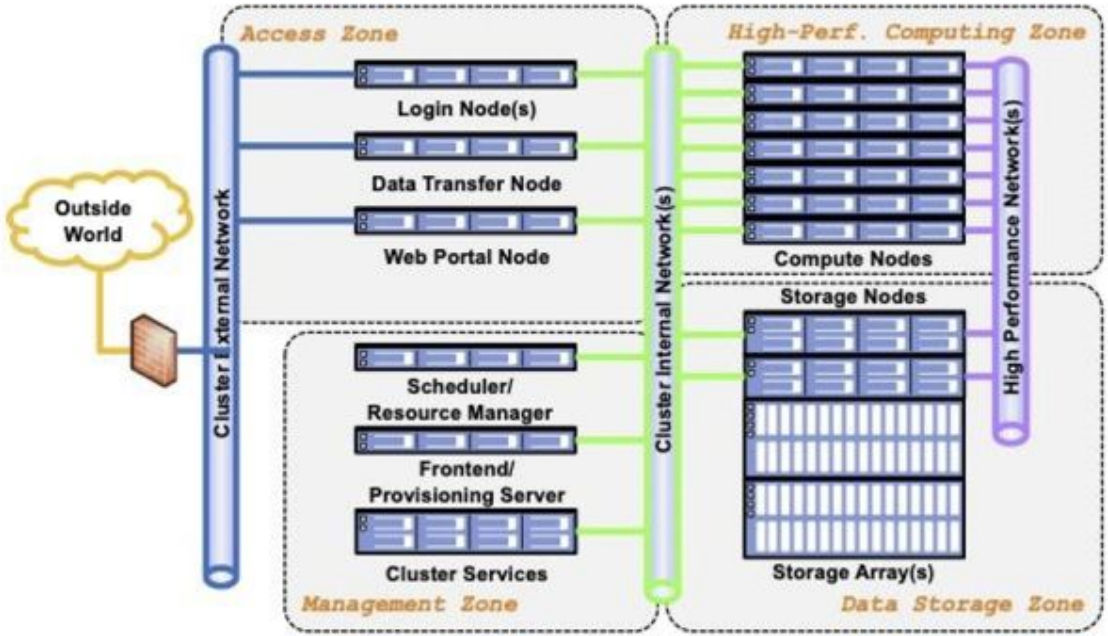


Fig. 1. HPC System Reference Model

NIST SP 800-223 HPC reference architecture – security questions:

- Management of data ingested at Tb/s (e.g. SKA example)?
- Back plane communications and control?
- Data archive functions?
- System backup and restore?
- Vendor access zone?
- ICAM (Identity, Credentials and Access Management) functions?

Complications – HPC and security:

1. Security needs to be built in, from the beginning: it's expensive to retro-fit.
2. HPC culture of speed as primary driver.
3. In the past, low attractiveness of HPC to malevolent actors.
4. However, the past is no longer applicable: hackers are now more sophisticated.
5. Existence proofs of malevolent hacking, e.g. Bitcoin mining, Gemini, ALMA, NASA.
6. ALMA opportunity operational cost put at $100 M/y; ~$270,000 per calendar day.
7. If capital investment of $1.4 billion for ~30 years, additional $130,000/day: ~$400,000/day.
8. Long durations (2 months, say $24 million) to restore to working and install controls.
9. Public information indicates deep issues, not just risks.
10. From the HPC community's perspective: there are many potential control actions.

(Our) Questions – HPC and security:

1. **During system planning and design, how to gain attention and recognition of security as a primary non-functional requirement?**
2. **How to address deep-seated cultural deficits?**
3. **How to 'frame up' the challenges for high level analysis and presentation to key decision-makers?**
4. **Given constrained budgets for investment in security control services, how to prioritise among myriad potential controls?**

Motivation

1 - 3 from SPDO experiences (DH) and SKA-SDP and L2L (NE).
4 from NIST SP 800-223, and participation in NIST HPC Security Working Group (DH).

Some answers: SABSA provides an analysis framework

Question	Some SABSA Answers
1. Gain decision-makers' attentions?	1. Recognise and communicate that risks and opportunities are inter-related
2. Address deep-seated cultural deficits	2. Talk in 'business' – or **'science outcomes'** – language
3. 'Frame up' the challenges for high level analysis and presentation ?	3. SABSA's attributes language
4. Prioritise among myriad potential controls?	4. Start with prioritising asset values at risk, then use attributes to identify likely vulnerabilities and potential impacts

Outline:

- Background: SKA; Listen to the Land.
- HPC: Speed above all; Special challenges.
- NIST SP 800-223: Complications; Questions; Some Answers.
- What is SABSA?
- SABSA in context: A linear programming construct.
- Summary: SABSA's benefits; A call to action.

What is SABSA?

Sherwood

- John **S**herwood: thought leader and Chief Architect of the SABSA model.

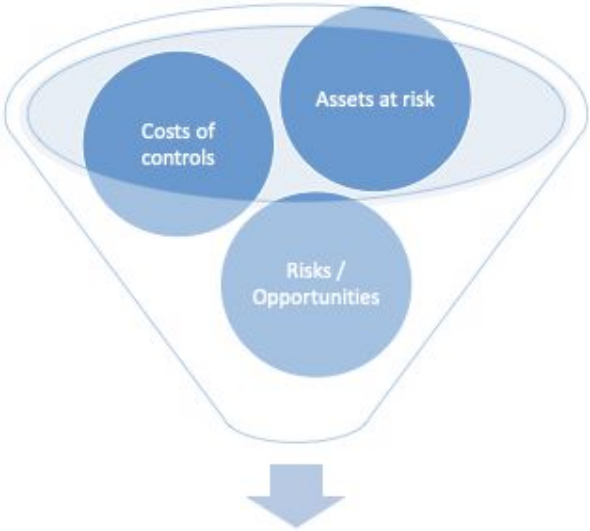
Applied

- A practicable, hands-on approach to align security architecture to business goals.

Business

Security

Architecture: People, Processes, Security services:

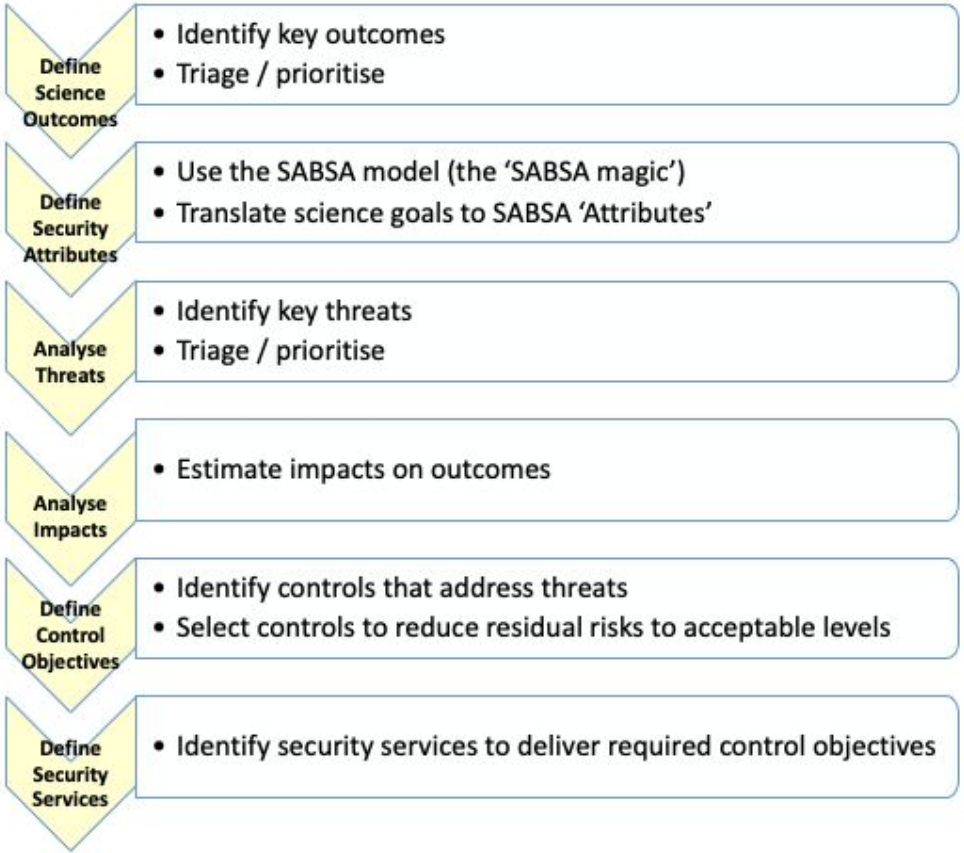


Prioritised security services that reduce risks to acceptable levels

Driven by business requirements (~ 'science outcomes')

X

The SABSA approach translated into S-HPC for science/engineering outcomes:



SABSA: Security architecture to align security services to science outcomes

X

SABSA's attributes are constantly under development, an example from 2009:

SABSA Business Attributes and Metrics

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
	User attributes. These attributes are related to the user's experience of interacting with the business system.		
Accessible	Information to which the user is entitled to gain access should be easily found and accessed by that user.	Soft	Search tree depth necessary to find the information
Accurate	The information provided to users should be accurate within a range that has been preagreed upon as being applicable to the service being delivered.	Hard	Acceptance testing on key data to demonstrate compliance with design rules
Anonymous	For certain specialized types of service, the anonymity of the user should be protected.	Hard Soft	Rigorous proof of system functionality Red team review*
Consistent	The way in which log-in, navigation, and target services are presented to the user should be consistent across different times, locations, and channels of access.	Hard Soft	Conformance with design style guides Red team review

	Management attributes. This group of attributes is related to the ease and effectiveness with which the business system and its services can be managed.		
Automated	Wherever possible (and depending upon cost/benefit factors) the management and operation of the system should be automated.	Soft	Independent design review

Business attribute	Attribute explanation	Metric type	Suggested measurement approach
Change-managed	Changes to the system should be properly managed so that the impact of every change is evaluated and the changes are approved in advance of being implemented.	Soft	Documented change management system, with change management history, evaluated by independent audit
Controlled	The system should at all times remain in the control of its managers. This means that the management will observe the operation and behavior of the system, will make decisions about how to control it based on these observations, and will implement actions to exert that control.	Soft	Independent audit and review against Security Architecture Capability Maturity Model†
Cost-effective	The design, acquisition, implementation, and operation of the system should be achieved at a cost that the business finds acceptable when judged against the benefits derived.	Hard	Individual budgets for the phases of development and for ongoing operation, maintenance and support
Efficient	The system should deliver the target services with optimum efficiency, avoiding wastage of resources.	Hard	A target efficiency ratio based on (Input value)/(Output value)

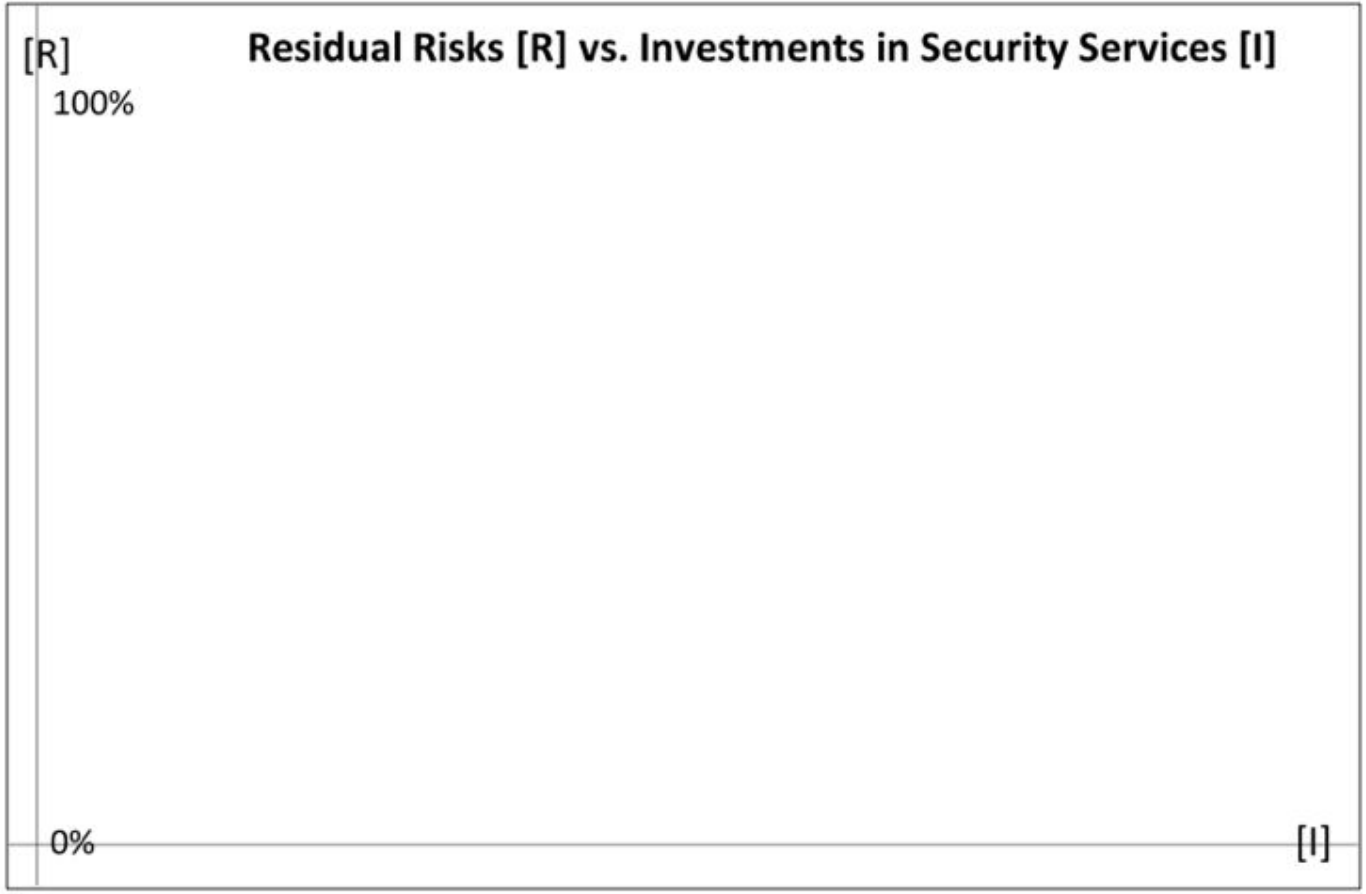
Further category examples: Operational, Risk, Financial, Human, Process . . .

X

Outline:

- Background: SKA; Listen to the Land.
- HPC: Speed above all; Special challenges.
- NIST SP 800-223: Complications; Questions; Some Answers.
- What is SABSA?
- SABSA in context: A linear programming construct.
- Summary: SABSA's benefits; A call to action.

A linear programming construct to visualise SABSA in context: 1 of 7

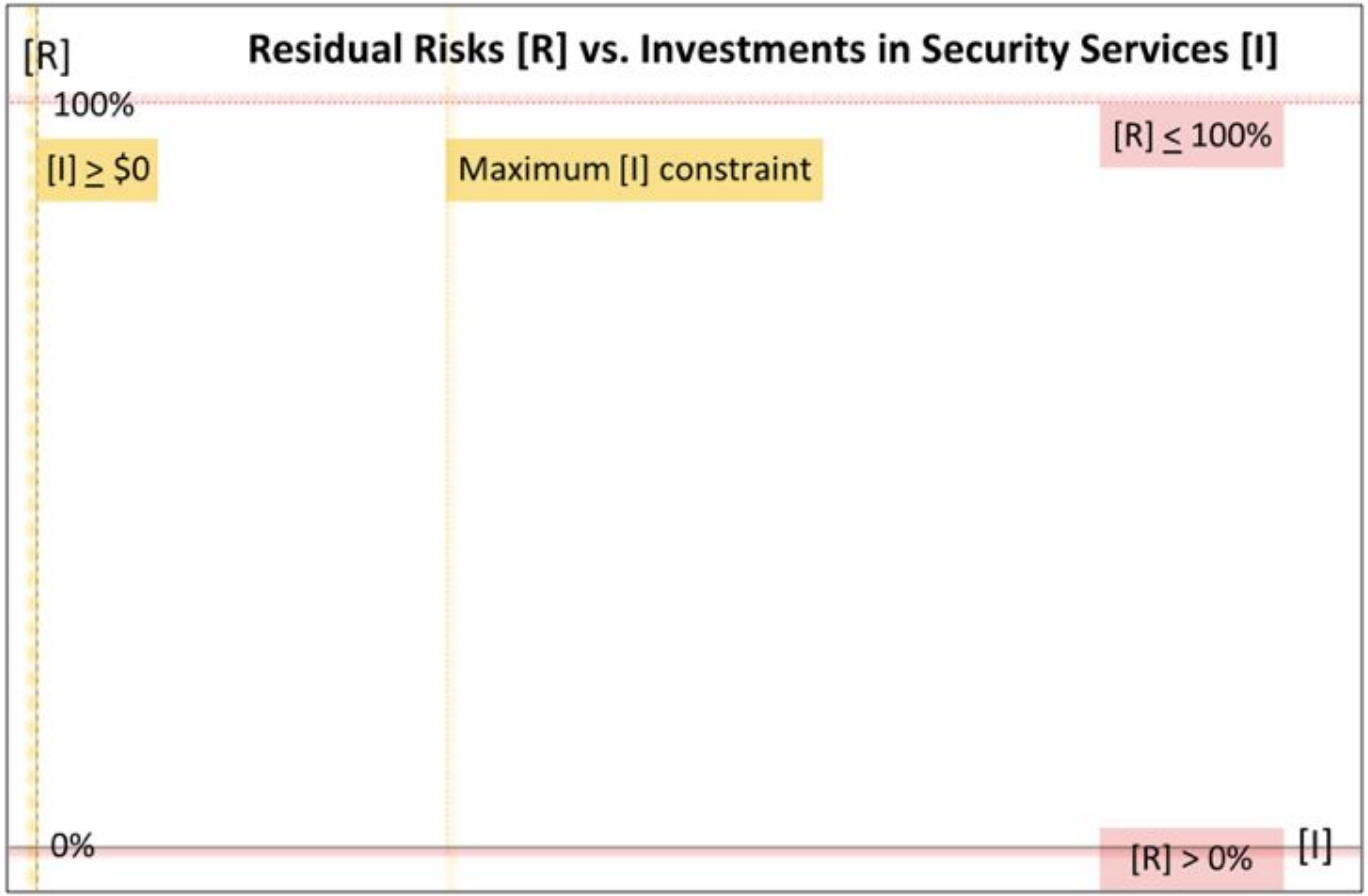


Setting up a visualisation of the trade-offs between [R] and [I]

Untreated [R] set at 100%; [R] can never be negative

No matter what the [I], there will always be some residual risk

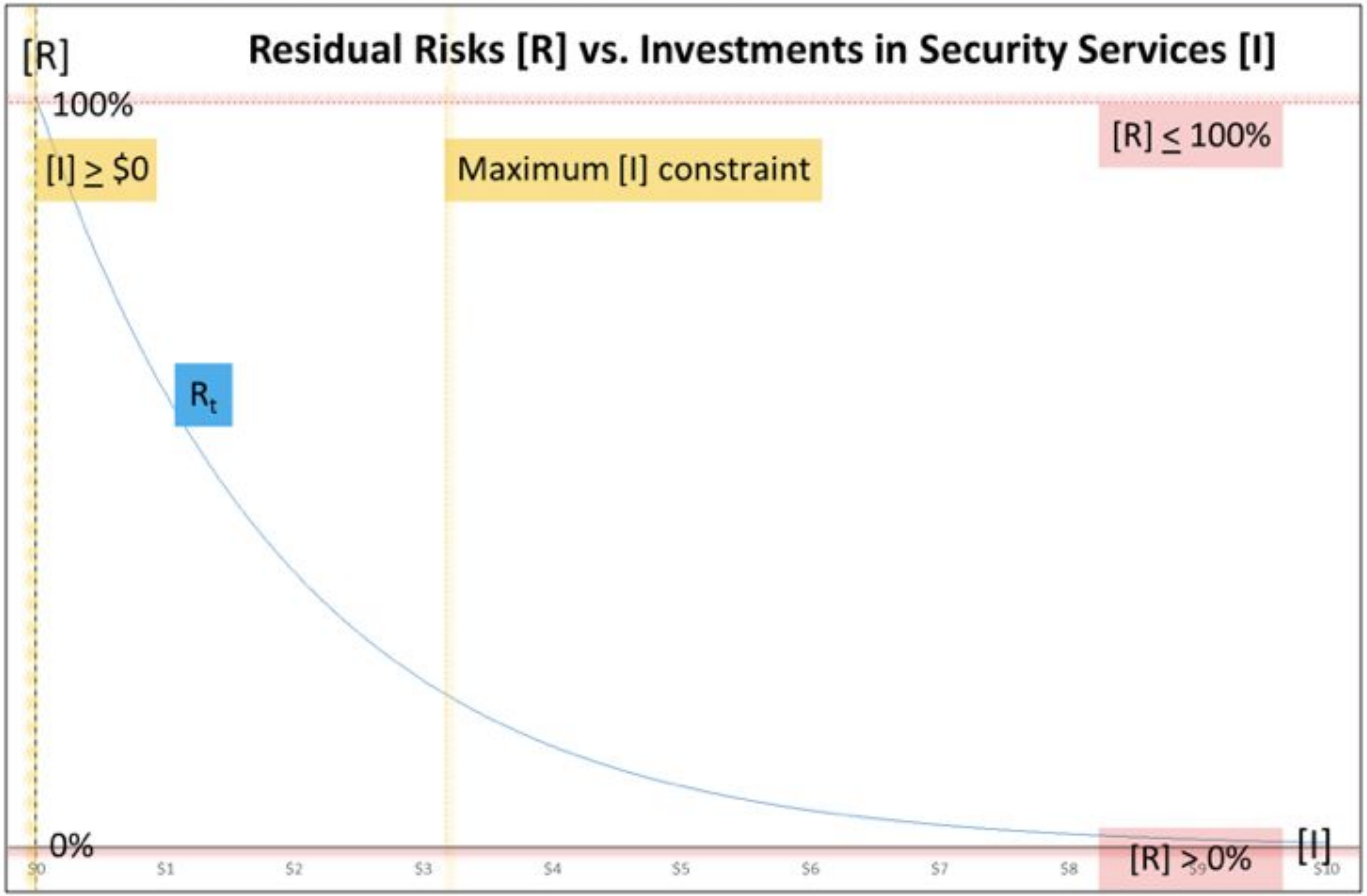
[I] can never be negative; there will always be a constraint on funds for [I]



As a soft constraint, increasing Maximum [I] usually requires Cost-Benefit justification

x

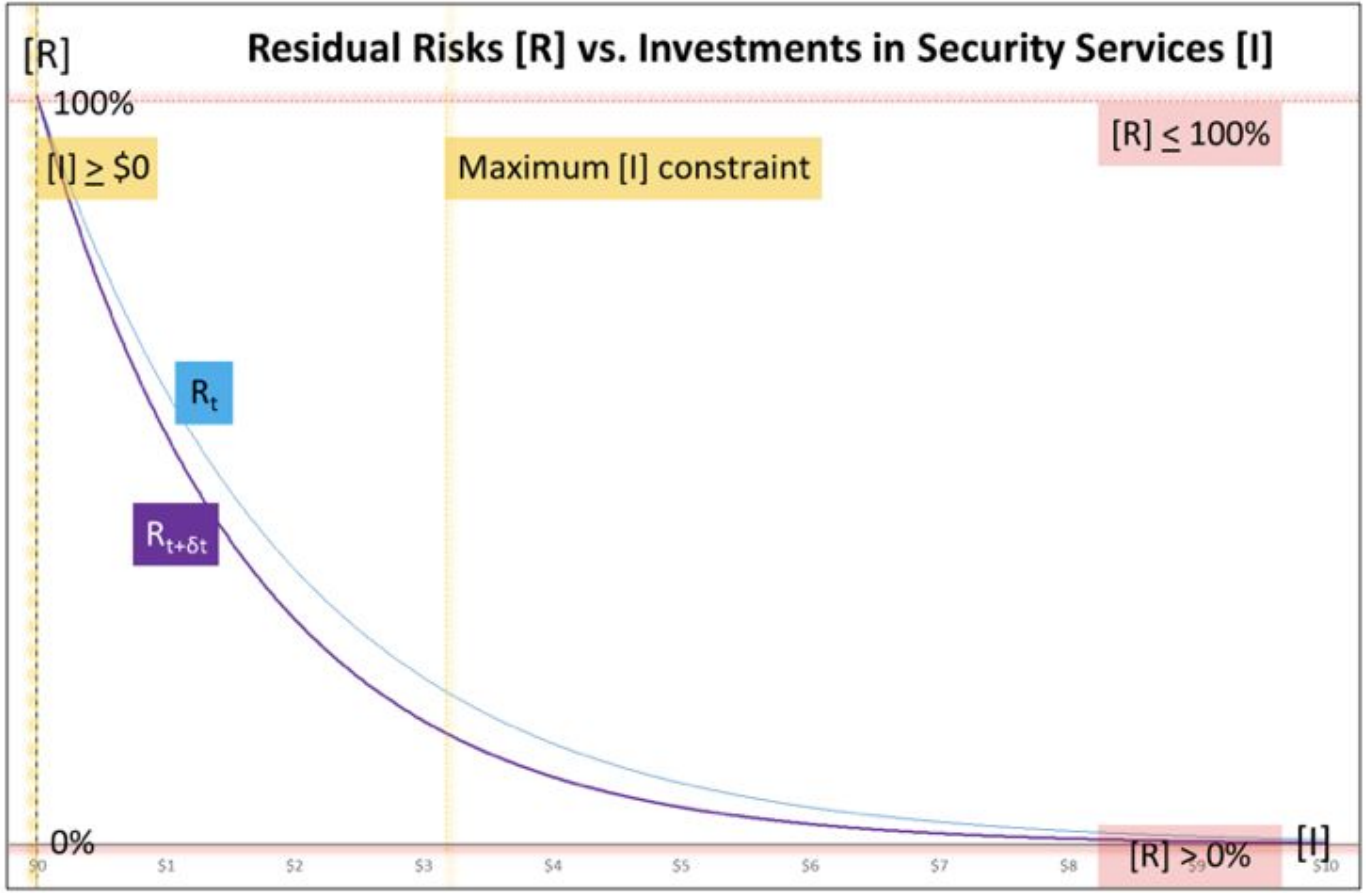
Increased [I] usually results in an ~exponentially reducing [R]



No matter what the [I], there will always be some residual risk

X

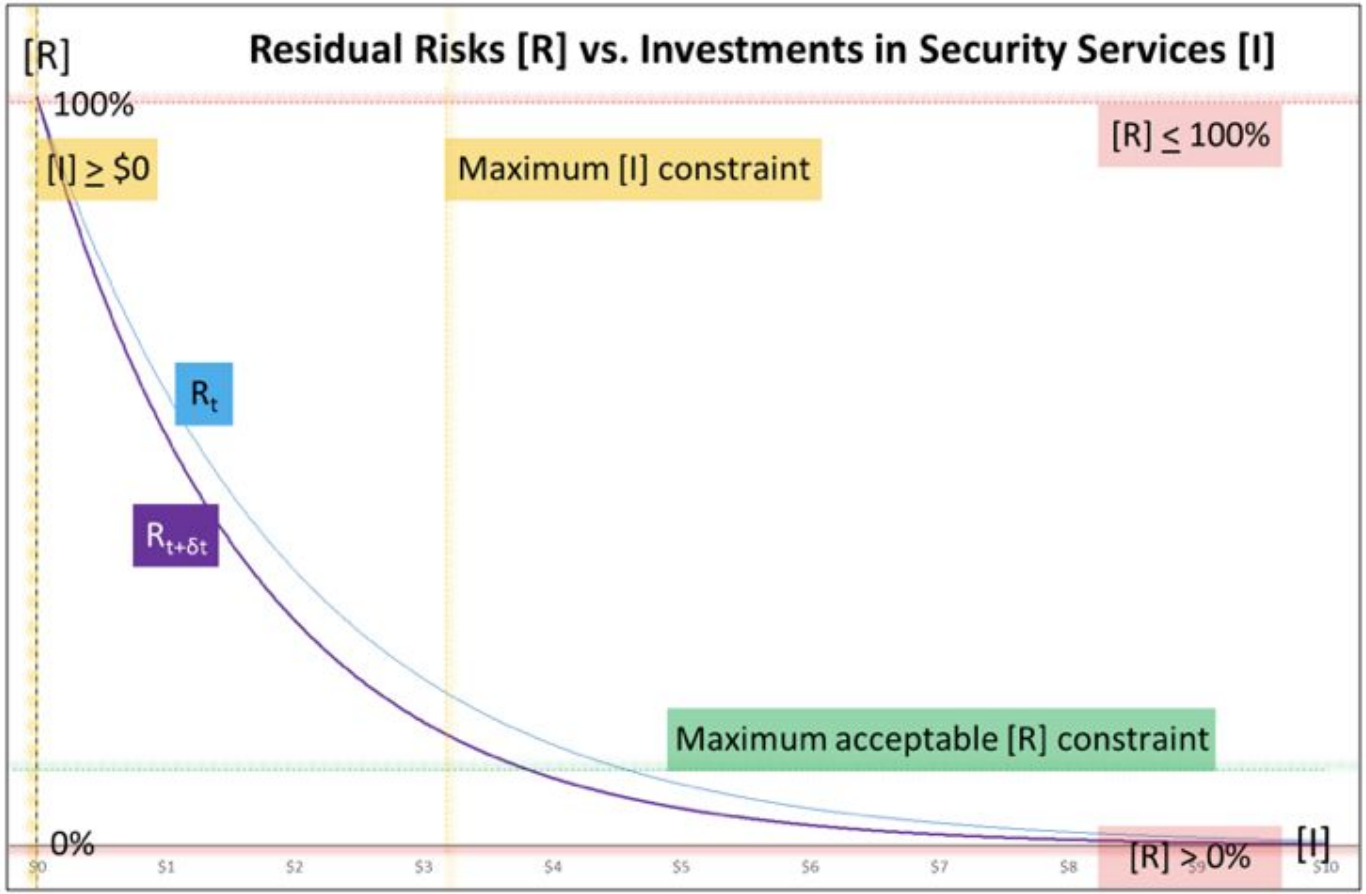
SABSA facilitates exploration of various Security Services to reduce [R] over time



In this example, after an incremental time δt, a lower [R] results for all [I]

X

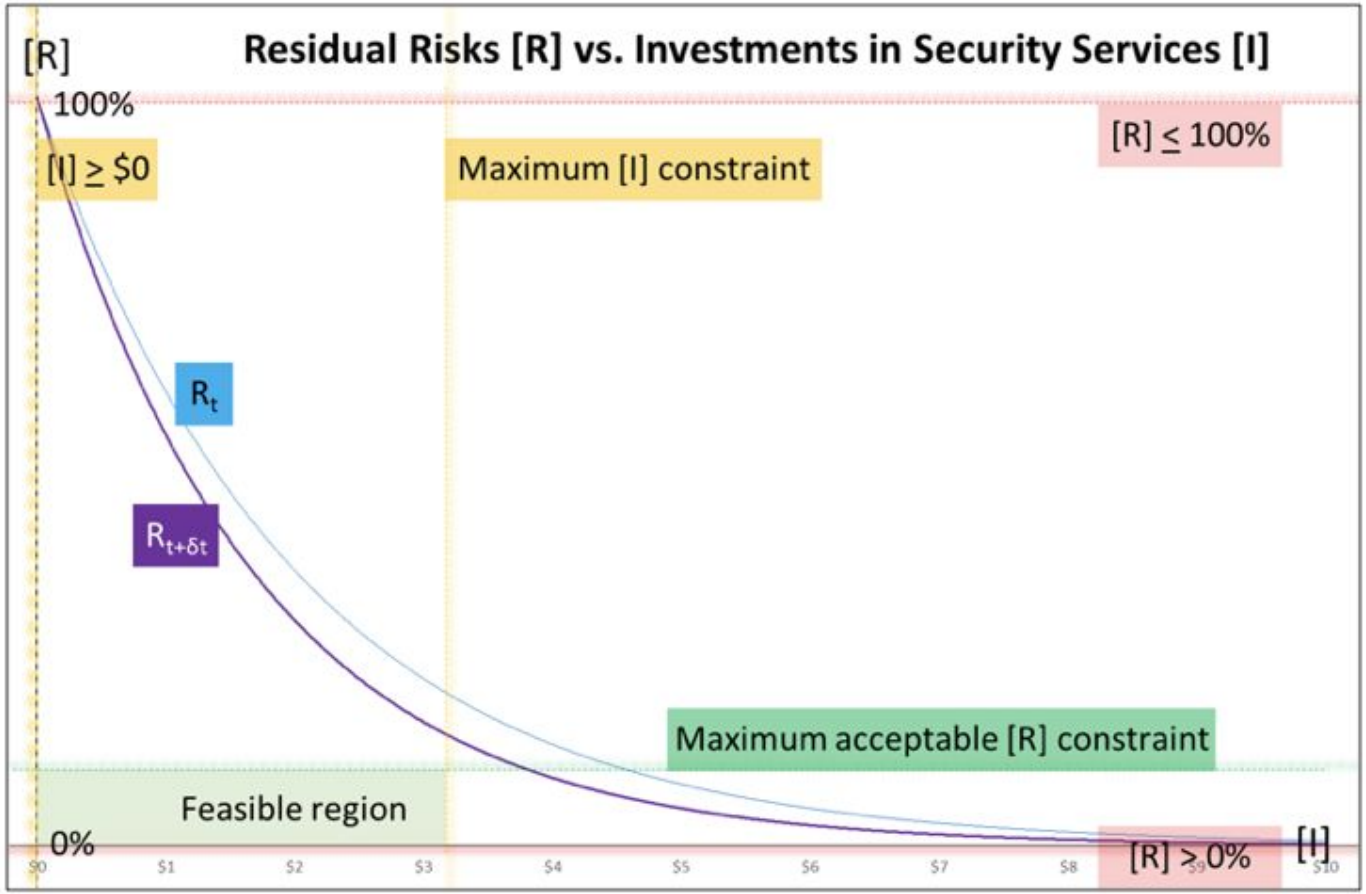
Key stakeholders must define their maximum acceptable [R]



Quantifying [R] can be difficult, however relative [R] is often more easily understood

X

Constraints define a 'Feasible region' as a target for prioritised [I] in Security Services



Requires increase in either Max[I] and/or Max[R]; or more effective Security Services

X

Outline:

- Background: SKA; Listen to the Land.
- HPC: Speed above all; Special challenges.
- NIST SP 800-223: Complications; Questions; Some Answers.
- What is SABSA?
- SABSA in context: A linear programming construct.
- Summary: SABSA's benefits; A call to action.

SABSA's benefits:

1. Focuses attention on highest priority assets.
2. Focuses attention on the most efficient portfolio of controls to reduce [R].
3. Identifies trade-offs for [I] vs [R].
4. Provides decision-makers traceability and rationale for commitment of [I].
5. Widely used in industry (outside the USA), e.g. finance, government services, defence and intelligence communities, standards bodies.
6. Training emphasises SABSA in practice, although theory is also addressed.
7. A vibrant practitioner community exists with two annual conferences:
   - COSAC Ireland (COSAC was originally COmputer Security And Controls).
   - COSAC Asia-Pacific.

Call to action:

1. COSAC community to reach out to NIST and HPC community ✓
2. SABSA to be presented at SC23 conference ✓
3. NIST and HPC folk to attend SABSA training?
4. NIST and HPC folk to participate in COSAC?
5. NIST to recommend SABSA (or equivalent) to optimise selection of cybersecurity controls?

Thank you!

2nd Annual Workshop on Cyber Security in HPC (S-HPC'23).
Collocated with the 35th Supercomputing Conference (SC23).
Sunday 12th November 2023.
Denver, CO, USA.

Information Security Controls Prioritisation: SABSA for HPC.

- Nicolás Erdödy (nicolas.erdody@openparallel.com)
- Duncan Hall (duncan.hall@ieee.org)