Accenture Response to

Request for Quotation – Attachment 3

Initial Risk Assessment

Accenture RFQ-CM-11257

24th August 2025

AEC
Australian Electoral Commission

Table of Contents

1 Introduction 3

2 Risk Management 4

2.1 Purpose 4

2.2 Application 4

2.3 Policy Principles 5

2.4 Awareness, Training & Induction 6

2.5 Review 6

2.6 Risk Management Process 6

2.7 Identification 7

2.8 Response & Mitigation 9

2.9 Initial Program Risk Register 10

2.10 Initial Transition-In Risk Register 17

Copyright © 2025 Accenture. All rights reserved.

1 Introduction

Accenture adopts a proactive, structured and transparent risk management framework that is embedded across all phases of the FAD Reform Program Solution lifecycle. This approach is fully aligned with the AEC's expectations, integrates seamlessly with the Delivery Management Office (DMO) functions and is supported by our extensive experience delivering complex ICT programs.

A core feature of our approach is the RAID governance model, maintaining a centralised register within the DMO. This register ensures visibility, traceability and accountability across Multi-Disciplinary Teams (MDTs). Our approach is collaborative by design, ensuring that risk management activities are aligned with the Australian Electoral Commission (AEC) policies and relevant Commonwealth frameworks. In particular, we draw on the ISO 31000:2018 Risk Management Standard, the Commonwealth Risk Management Policy and the AEC's Risk Management Policy Framework to create a robust and fit-for-purpose framework.

Risk management is embedded into the program's governance cadence, including PI planning sessions, sprint retrospectives and program steering meetings, ensuring regular review, escalation and resolution of risks. Lessons learned from previous delivery are systematically applied to refine and strengthen risk identification and mitigation processes, supporting continuous improvement throughout the engagement.

From project commencement, we will work closely with the AEC to:

- Define program-specific risk likelihood and impact criteria for the FAD program as part of mobilisation, ensuring alignment with AEC's Enterprise Risk Management framework, its governance requirements and evolving program needs.
- Establish and apply agreed criteria for identifying, categorising, prioritising and treating risks, with treatment and remediation actions focused on risks that exceed the agreed risk appetite.
- Implement additional protections and classification treatments as required for specific incidents or sensitive activities.
- Embed a culture of proactive risk ownership and accountability, ensuring the Project Team, DMO, MDT and other stakeholders are aware of and understand their responsibilities in managing risks.
- Track, review and report risks at agreed intervals to maintain transparency and enable timely decision-making.

Copyright © 2025 Accenture. All rights reserved.

2 Risk Management

2.1 Purpose

The Initial Risk Assessment serves as a key mechanism for the AEC to assess:

- Our understanding of the FAD Solution delivery environment and its inherent challenges.
- Our ability to anticipate, prioritise and mitigate risks across technical, operational and stakeholder domains.
- The maturity of our delivery governance and alignment with the AEC's risk posture.

This submission demonstrates not only our ability to identify risks but also our capability to apply practical, proven mitigation strategies grounded in experience from similar large-scale programs. The assessment has been prepared in full compliance with the AEC's Enterprise Risk Assessment Framework, applying:

- Standardised likelihood and consequence scales.
- Defined risk categories (strategic, operational, technical, compliance).
- The AEC's required formatting and submission templates.

These activities will be conducted within the governance, escalation and reporting mechanisms outlined in the AEC's Risk Management Framework, including alignment to the three layers of Risk Governance, Risk Operation and Risk Culture. This will be achieved in close collaboration with the Australian Electoral Commission (AEC), ensuring that risk management activities are aligned with AEC's risk appetite, escalation protocols and enterprise reporting requirements, while also adhering to the FAD Program's objectives and the principles as defined in ISO 31000:2018.

By combining our internal RAID management discipline with the AEC's risk tools, including the s 47E(d) and risk acceptance escalation table, we ensure complete consistency, traceability and transparency in the management of program risks. This allows to contribute to the AEC's broader strategic and enterprise risk oversight objectives.

2.2 Application

The Risk Management policy applies to all Accenture personnel, contractors, delivery partners and stakeholders contributing to the FAD Solution. It extends to the management of shared risks that cross organisational boundaries or involve external agencies, sectors or jurisdictions where dependencies may affect delivery outcomes.

The application of this framework is underpinned by:

- A central RAID register maintained by the DMO, capturing and tracking all identified risks, assumptions, issues and dependencies.
- Clear assignment of risk ownership across DMO, MDTs and enabling teams to ensure accountability.
- Engagement of specialist governance teams for selected risk types is advised, ensuring SMEs have visibility where necessary (e.g. security risks will require engagement with AEC Cyber; privacy risks will require engagement with the Legal & Privacy Officer, Financial/commercial risks will require engagement with procurement, etc.)
- Engagement of specialist governance teams for selected risk types is advised, ensuring SMEs have visibility where necessary (e.g. security risks will require engagement with AEC

Copyright © 2025 Accenture. All rights reserved.

Cyber; privacy risks will require engagement with the Legal & Privacy Officer, Financial/commercial risks will require engagement with procurement, etc.)

- Integration of risk management into strategic planning, business case development, delivery governance forums and operational processes.

This approach fosters a culture where risk ownership is embedded at every level, ensuring that risks are actively monitored, regularly reviewed and continuously refined in line with the program needs. We provide tailored security awareness programs in line with AEC for newly onboarded project team members and refreshers for current members. This would ensure consistent understanding and proactive engagement from the outset. Risk appetite is a key element of the approach to the management of risk and is defined as the amount and type of risk that AEC is prepared to seek, accept or tolerate in relation to this program. The risk appetite would be determined by the Governance bodies and captured within the Risk Management Policy.

2.3 Policy Principles

Accenture's risk management policy is aligned with ISO 31000:2018 Risk Management standards and is fully integrated within AEC's Enterprise Risk Management Framework. This alignment ensures that risk is managed consistently across strategic, enterprise and operational levels in line with the Commonwealth Risk Management Policy and AEC governance expectations. The FAD solution delivery will focus on these principles to support the three layers of the AEC's Risk Management Framework, Risk Governance, Risk Operation and Risk Culture. This will help ensure adequate decision-making, reporting and continuous improvement is at the forefront.

The principles guiding this policy are:

- **Create and protect value:** Risk management actively supports delivery outcomes and emphasises embedding risk into all decision-making activities.
- **Integration:** Embedded into planning processes, delivery processes and consistent with the AEC's enterprise-wide approach to risk management.
- **Support decision-making:** Provides a structured basis for prioritising actions and allocating resources and escalating risks in accordance with the AEC Risk Acceptance and Escalation Table.
- **Address uncertainty:** Considers both threats and opportunities, including strategic, enterprise and shared risks as defined in the AEC Risk Management Framework.
- **Systematic and timely:** Applies structured, repeatable methods in line with the AEC Risk Management Guidelines to ensure efficiency and consistency.
- **Best available information:** Informed by reliable data, stakeholder engagement and expert judgement to allow for evidence-based decision-making.
- **Tailored to context:** Adapted to the FAD solution's scope, scale and complexity, while meeting AEC specific risk appetite and tolerance thresholds.
- **Human and cultural considerations:** Reinforces the AEC's positive risk culture by recognising the role of people and organisational behaviour in effective risk management.
- **Transparency and inclusiveness:** Promotes open communication and collaboration with stakeholders across the program and within AEC governance forums.
- **Continuous improvement:** Leverages lessons learned, monitoring and review activities to continually enhance risk management capability.

Copyright © 2025 Accenture. All rights reserved.

By embedding these principles into the FAD solution delivery, risk management becomes an integrated, transparent and value addition component of program governance while aligning fully with the AEC's Enterprise Risk Management Framework.

2.4 Awareness, Training & Induction

Accenture will run a mandatory training and awareness program for all staff involved in the AEC FAD program, supporting the broader framework of proactive risk ownership outlined in this policy. The training will provide guidance on the appropriate use of supporting tools and templates to ensure a consistent and effective approach to risk management.

The induction program for new staff will include mandatory risk and compliance training, ensuring that all personnel understand their responsibilities, accountabilities, and expectations in managing program risks from the outset. All current personnel will be required to complete annual refresher training to maintain awareness and alignment with evolving program needs. Training completion will be actively tracked and monitored to ensure full participation and compliance across the program workforce.

2.5 Review

The Risk Management Framework will be reviewed regularly to ensure its ongoing relevance, effectiveness and alignment with the AEC Enterprise Risk Management Framework. Reviews will align to the AEC's established mechanisms for monitoring, evaluating and improving risk management at both the strategic and enterprise levels.

Reviews will leverage the AEC's governance and reporting structure, including:

- **Governance committee reporting:** relevant status will be recorded in the AEC's centralised Risk Register s 47E(d) and reported through relevant AEC Governance Committees, ensuring senior leadership oversight and decision-making in accordance with the Risk Acceptance and Escalation Table.
- **Framework effectiveness assessment:** Effectiveness will be evaluated using the AEC's approved mechanisms, such as internal control self-assessment and participation rates in risk training and workshops.
- **Strategic and enterprise risk integration:** Reviews will consider the alignment of project-level risks to the AEC's strategic and enterprise risks, ensuring appropriate escalation, resourcing and inclusion in enterprise-level reporting.

This multi-layered review process ensures alignment with the AEC's Risk Framework, along with staying consistent, transparent and continuously improving the processes throughout the FAD solution lifecycle.

2.6 Risk Management Process

This outlines the processes for dealing with risks during the implementation and operation of the AEC FAD Reform Program. This process covers activities consisting of the following:

- **Risk Identification:** Identification of risks to the Project
- **Risk Assessment:** Assessment of the identified risks, their impacts and mitigation strategies
- **Risk Response & Mitigation:** Prioritisation of risks and implementing risk-reduction procedures and treatment plans
- **Risk Monitoring:** Implementing a regular monitoring process for the identified risks as well as identification of new risks.

Copyright © 2025 Accenture. All rights reserved.

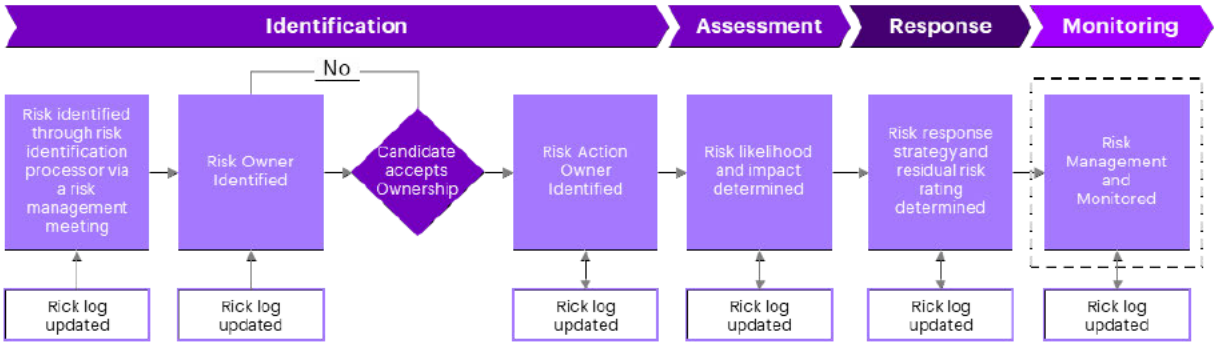


Figure 1: Risk Management Process

2.7 Identification

A risk is an event which is yet to eventuate and possess a threat to the outcomes of the project affecting schedule, budget or quality of the outcomes as described below:

- **Schedule:** results in slippage of project timelines.
- **Budget:** results in higher projected spending than planned.
- **Quality:** results in product not meeting business needs/expectations.

When a risk is identified that could have one or more of the above impact areas, it should be logged in the Risk Register. The first exercise of the risk logging process is the determination and development of the risk statement and description.

It is important to understand the risk before it is logged and the simplest way to do this is through the creation of the risk statement. The illustrations below provide an example of a project risk statement and an operational risk statement.

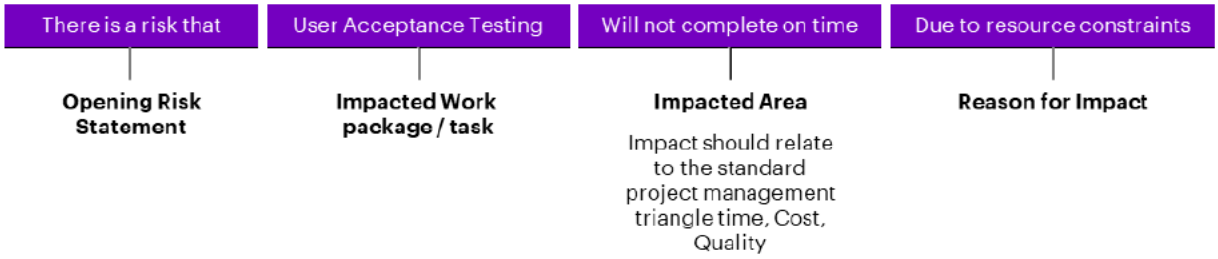


Figure 2: Project Risk Statement

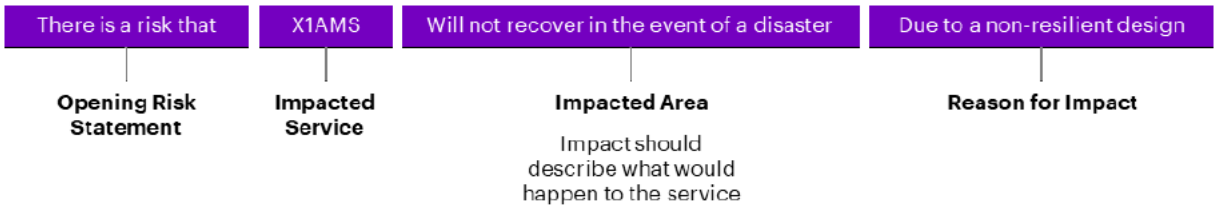


Figure 3: Operational Risk Statement

Following the creation of the risk statement, at a minimum the following areas must be detailed to allow for the risk to be assessed effectively.

Copyright © 2025 Accenture. All rights reserved.

The below components form the overall description of the risk; without these items a risk cannot be effectively managed				
Summary	**Event**	**Description**	**Trigger**	**Consequence**
The title should be punchy, however it needs to align with the structure outlined within this document: *<Opening> impact> <Impacted Area> <Impact Reason>*	Additional information about what the risk is and what would happen (event) if it occurred	Additional background to the risk including key terms and projects / services / teams involved	The trigger(s) should be short and concise. Triggers detail what could cause the risk to become an issue	The consequence is the result of the risk if it becomes an issue

Figure 4: Components to manage Risk

Based on the above, we recommend the following details should be documented against each risk in the Risk Register:

- **Risk Number:** Unique identifier of the risk
- **Risk Type:** Type of Risk classified as People, Process, Technology, Delivery.
- **Risk Title:** A statement explaining the risk
- **Risk Statement:** Should follow a cause-risk/event-impact/consequence construct.
- **Status:** Active/Retired/Mitigated/Mitigated with Residual Risk
- **Controls / Mitigation:** Actions to reduce the probability of or consequences of a threat
- **Residual Likelihood:** likelihood of occurrence after implementing the mitigating actions
- **Severity:** How severe the impact will be after implementing the mitigating actions
- **Residual Risk score:** A qualitative score that is more granular than inherent risk
- **Responsible Party:** Organisation who "owns" the risk (AEC or Accenture) and will drive the response to the risk
- **Owner:** Person (from AEC or Accenture) who is responsible for responding to the risk
- Date when Risk is logged – the date when risk has been identified
- **Due Date:** by which Risk should be resolved to avoid an impact on the project
- **Running Comments:** Each comment should be dated with the Author's name and should document progress, key discussions & actions

2.7.1 Risk Assessment

Once a Risk is identified and logged, it should be assessed to determine how it could affect the project in terms of schedule, budget or quality.

Severity of its impact should be determined and graded into High (H), Medium (M), Low (L). The exact quantification of what drives the Severity grading will be based on judgement of the Risk Owner and the corresponding quantification should be provided where possible in the Commentary against the risk.

Similarly, Likelihood should be graded into High (H), Medium (M), Low (L). Risk Score would define how the Response actions are prioritised relative to other Risks. Generally, the combination of Likelihood & Severity will drive the Score. The below matrix can be used as a guide:

Copyright © 2025 Accenture. All rights reserved.

Risk Likelihood	Risk Severity		
	Low	Medium	High
Low	Low	Medium	Medium
Medium	Low	Medium	High
High	Medium	Medium	High

Table 1: Calculation of Risk Score

2.8 Response & Mitigation

Risks can have one or multiple mitigations. Responses to a Risk could be:

- **Prevent:** Prevent the potential for the risk altogether to eliminate the cause or trigger itself.
- **Reduce:** Reduce the severity and/or the likelihood of the risk.
- **Accept:** Whereby no action is taken, and impacts are absorbed by the project. Usually this is an option for a small number of low Severity Risks.
- **Contingency:** Build in a contingency for that particular risk. This typically applies to schedule risks, whereby we would allow for extra time for a task.
- **Transfer:** Agree with another party to carry the risk.

These responses need to be factored into the Severity and Likelihood, which will then lead to the Residual risk score. This is the Risk Score that resides after mitigation of the risk, which will be used to prioritise the risks.

2.8.1 Risk Monitoring

Risk monitoring will occur as an ongoing practice, integrated into the overall program delivery oversight. As a standard practice, a weekly delivery review meeting will be conducted to review project progress, track open risks, agree on mitigation actions and assign clear ownership for those actions.

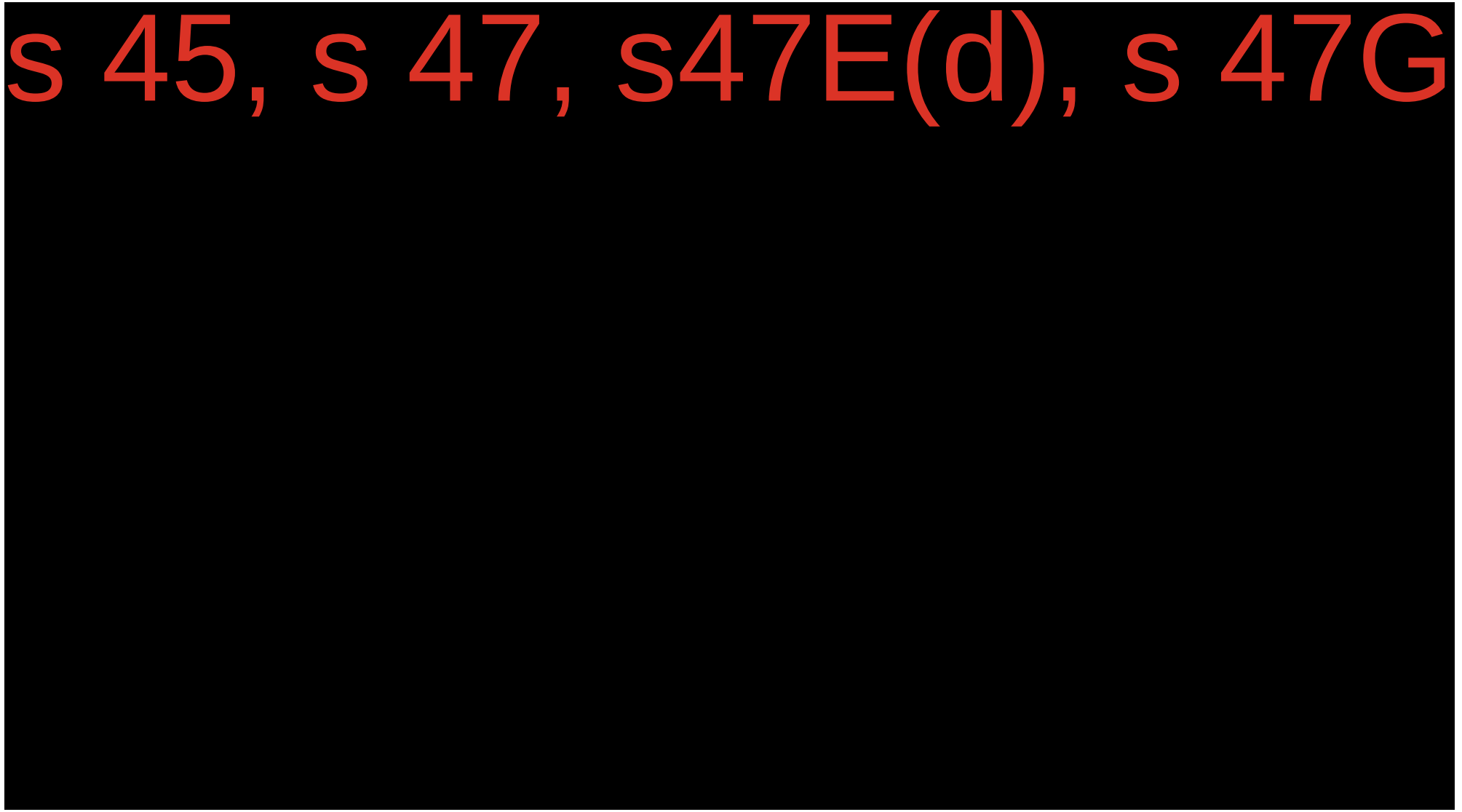
Risk Scores described above will be highlighted in ongoing project status reports to executive management. Risks will also be visible through the central RAID register which will be maintained by the DMO and shared with the AEC to provide up-to-date tracking of risk status, ownership and treatment progress.

In addition to weekly reviews, monthly sessions with senior leadership will be held to identify and log any emerging risks, ensuring the RAID register remains current and comprehensive. This approach ensures all relevant stakeholders have transparent, timely visibility of risks, understand their context and can take proactive measures to address them accordingly.

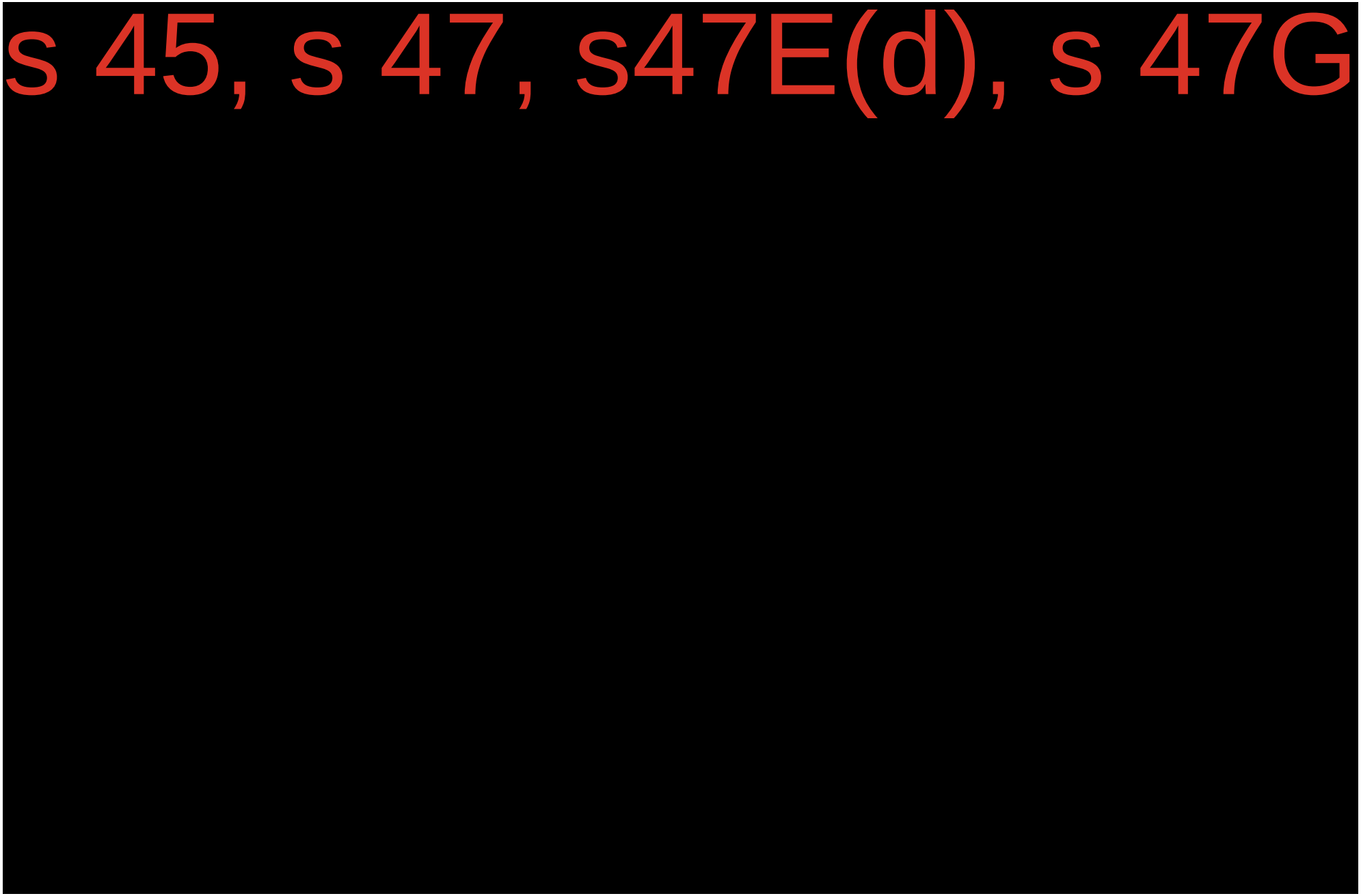
Copyright © 2025 Accenture. All rights reserved.

2.9 Initial Program Risk Register

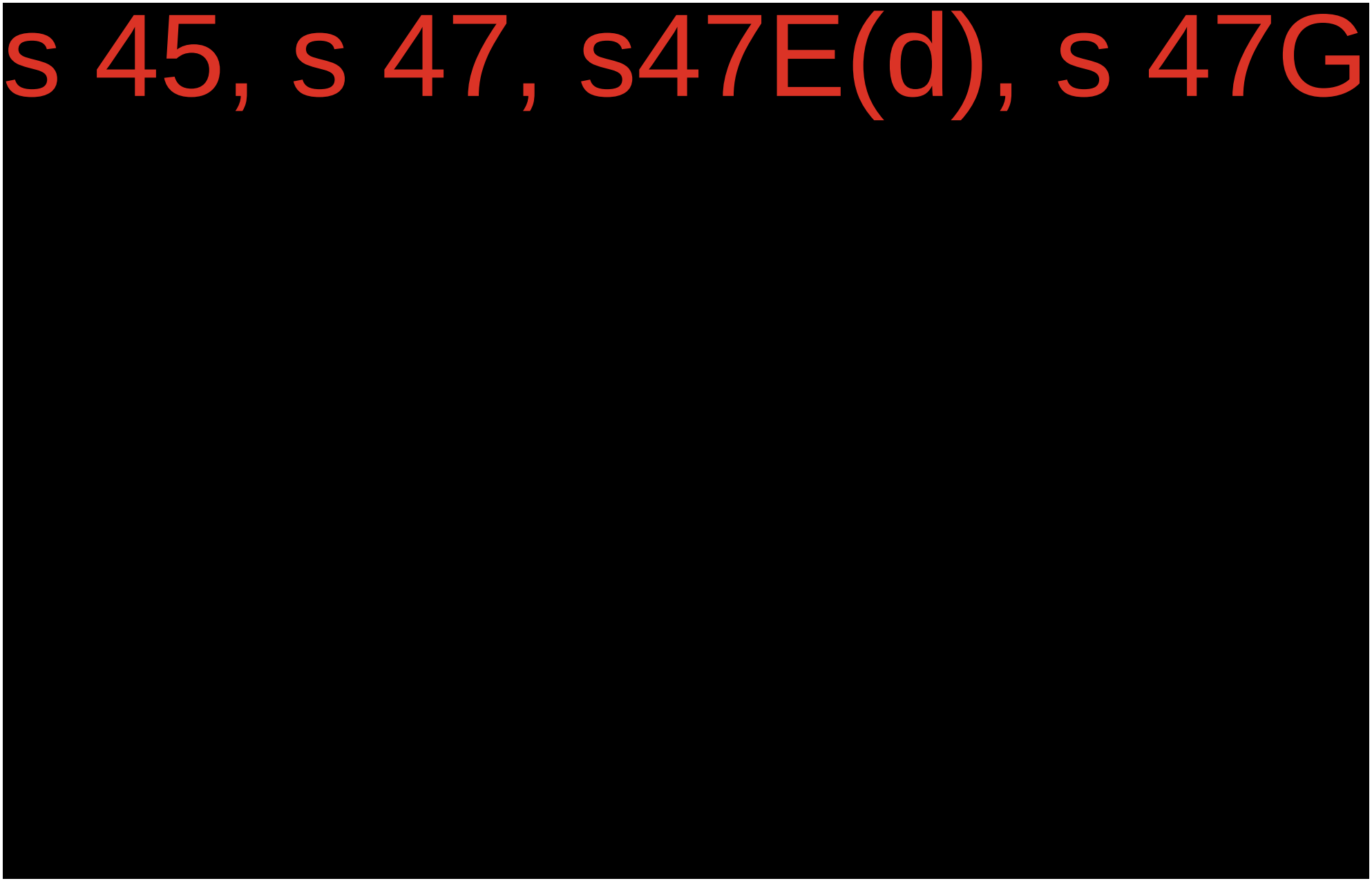
The table below describes the initial Risk Register with the risks as we see that at this stage. We would seek to work through these risks with AEC during contract negotiations and during the project to keep them relevant and up to date.



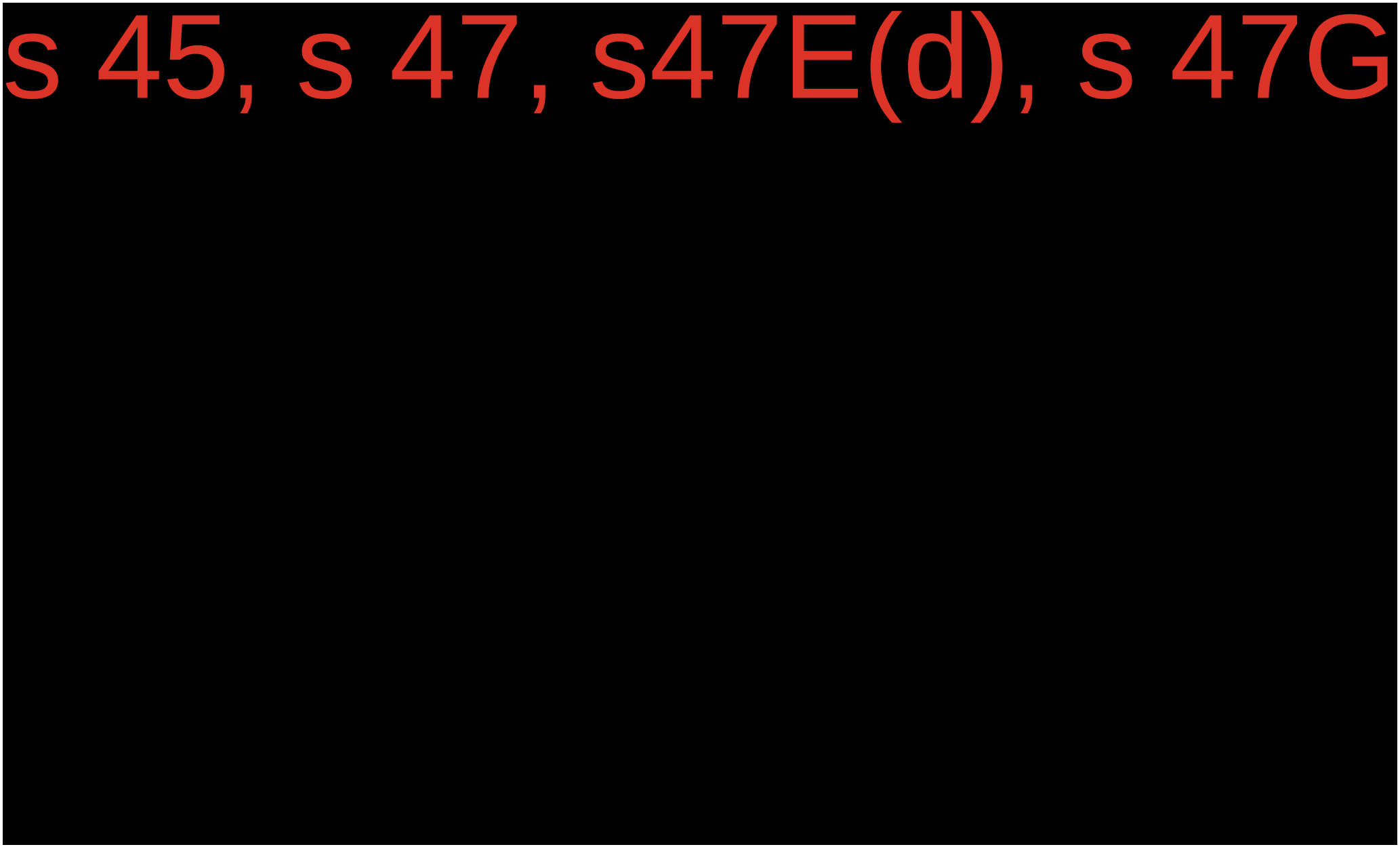
Copyright © 2025 Accenture. All rights reserved.



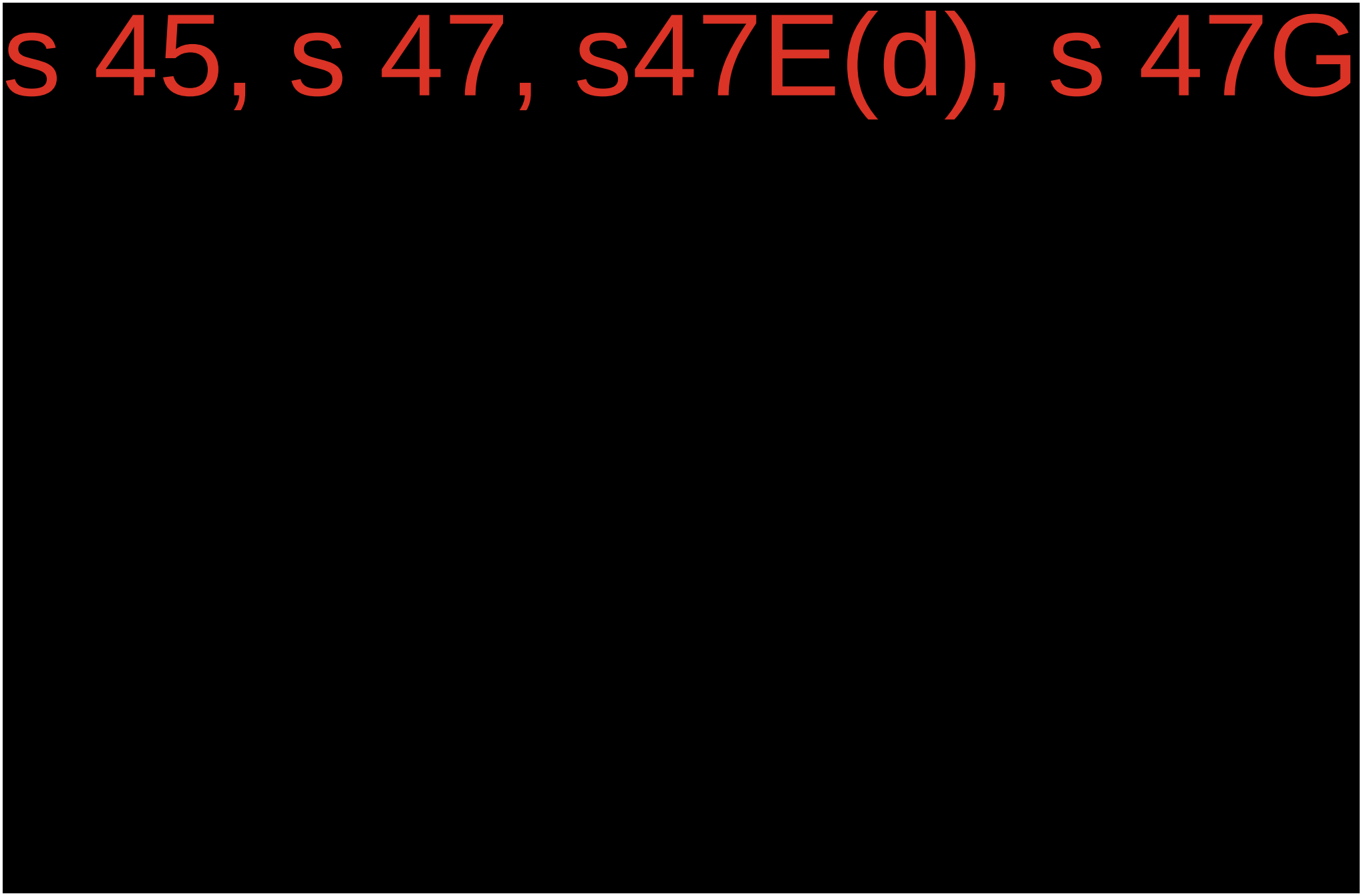
Copyright © 2025 Accenture. All rights reserved.

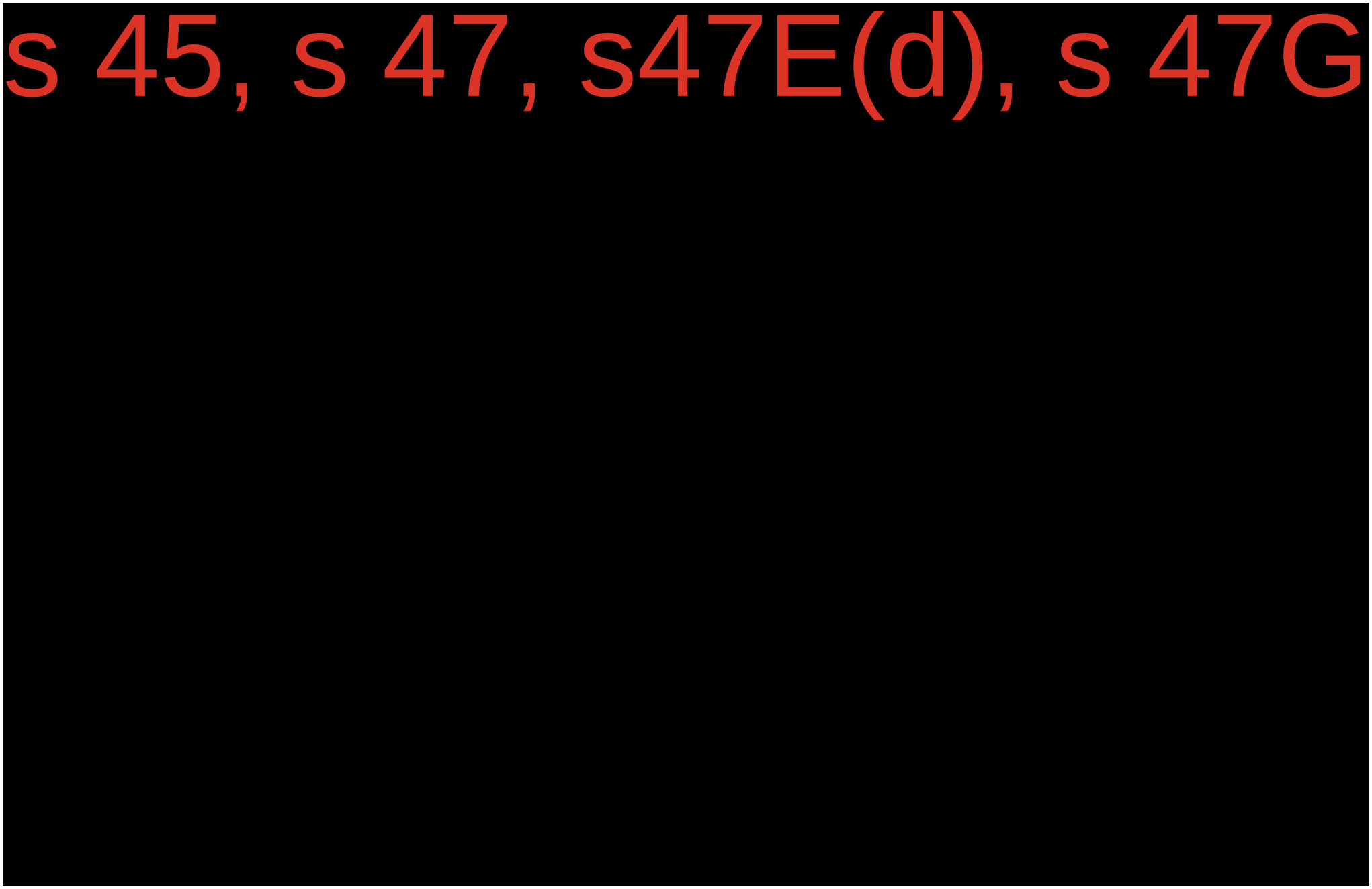


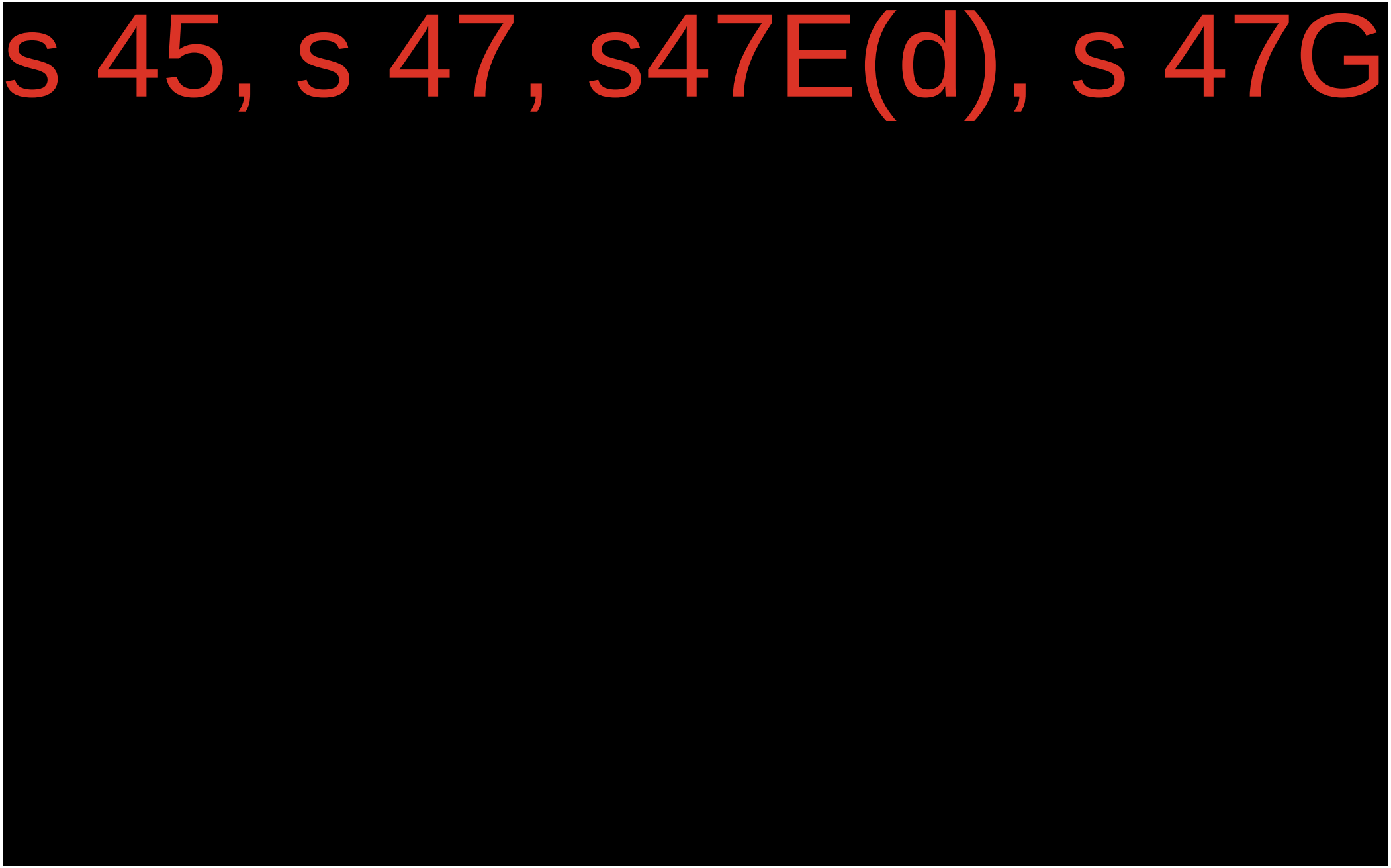
Copyright © 2025 Accenture. All rights reserved.



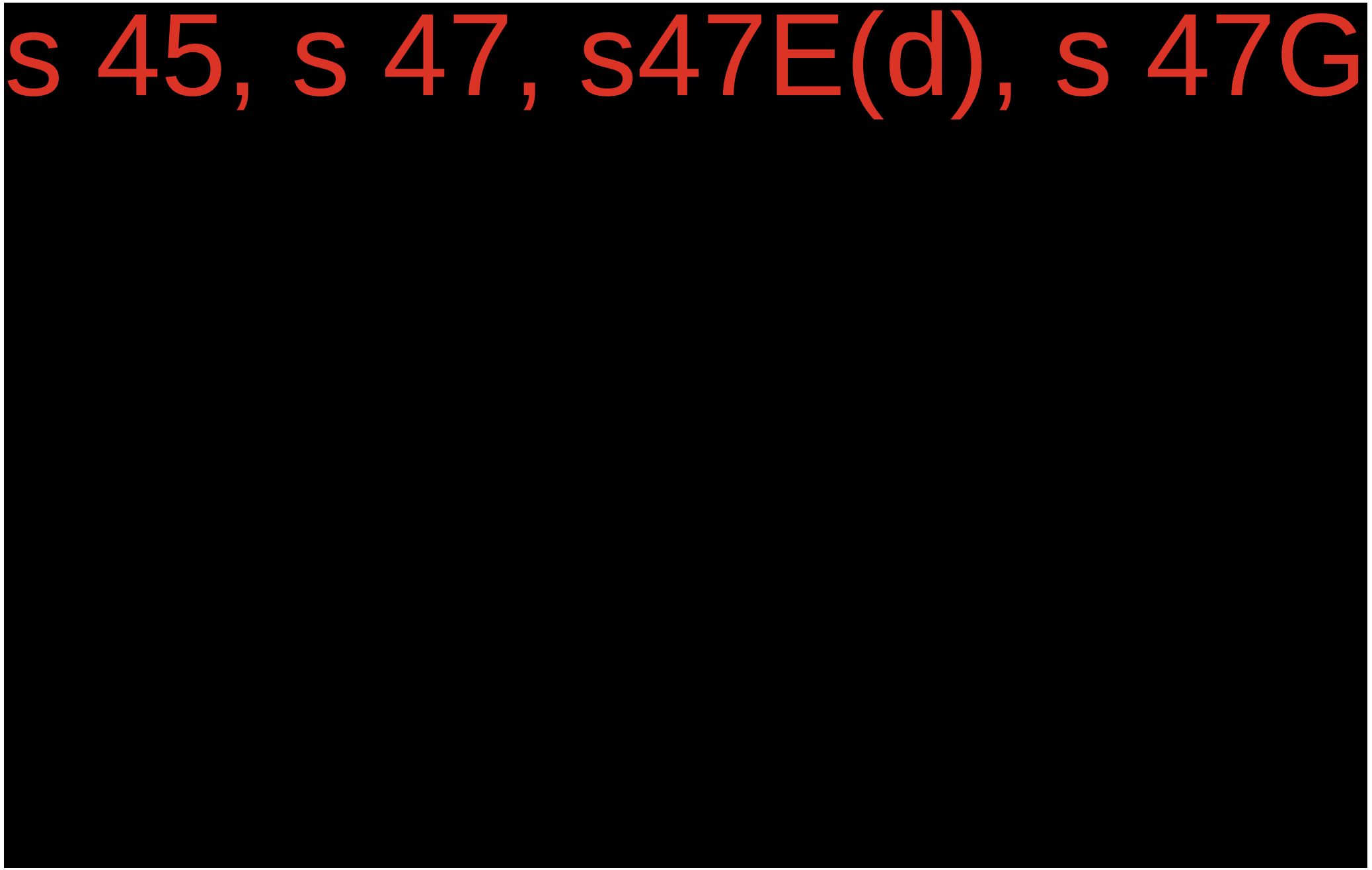
Copyright © 2025 Accenture. All rights reserved.


s 45, s 47, s47E(d), s 47G

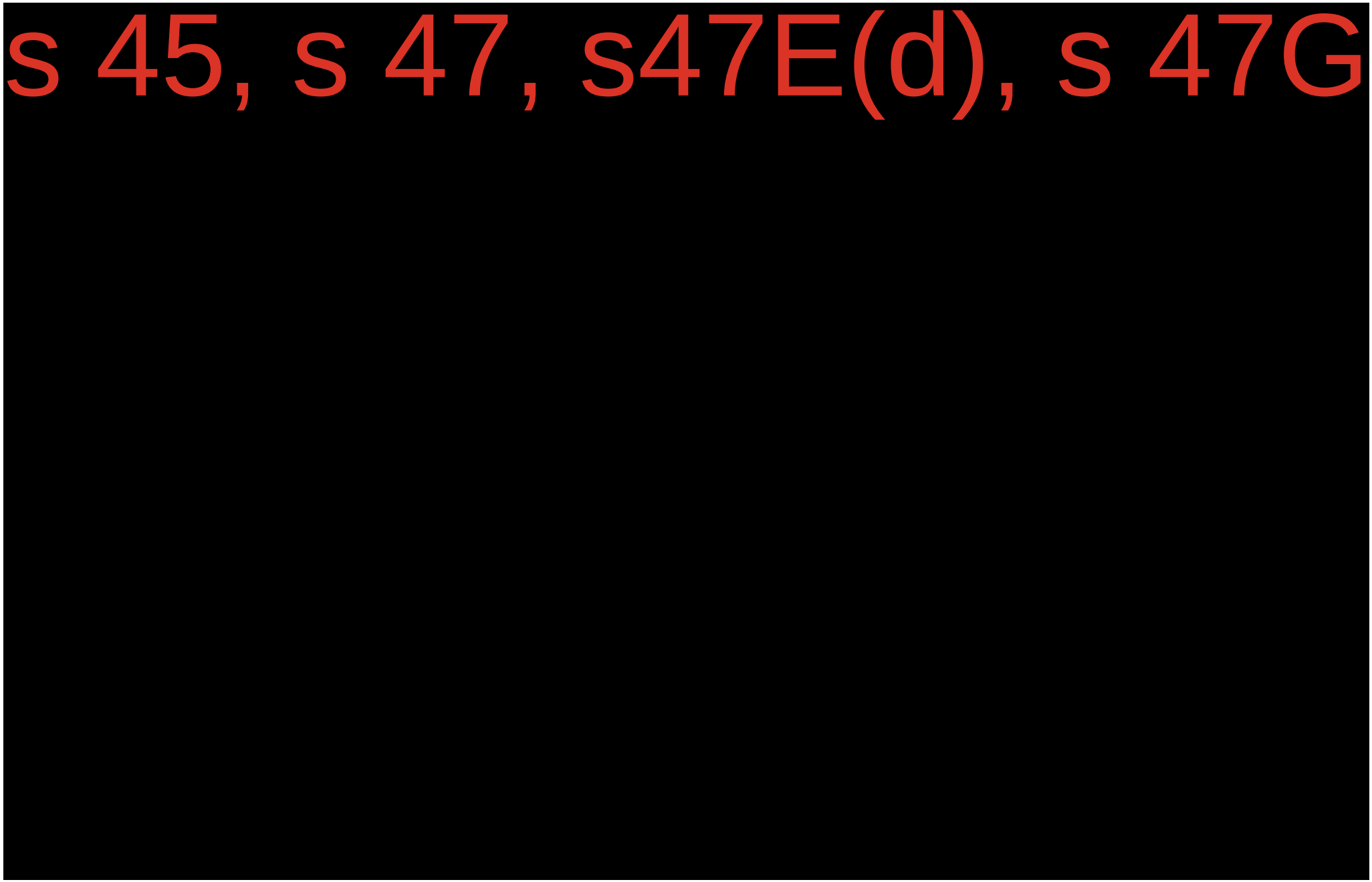

s 45, s 47, s47E(d), s 47G



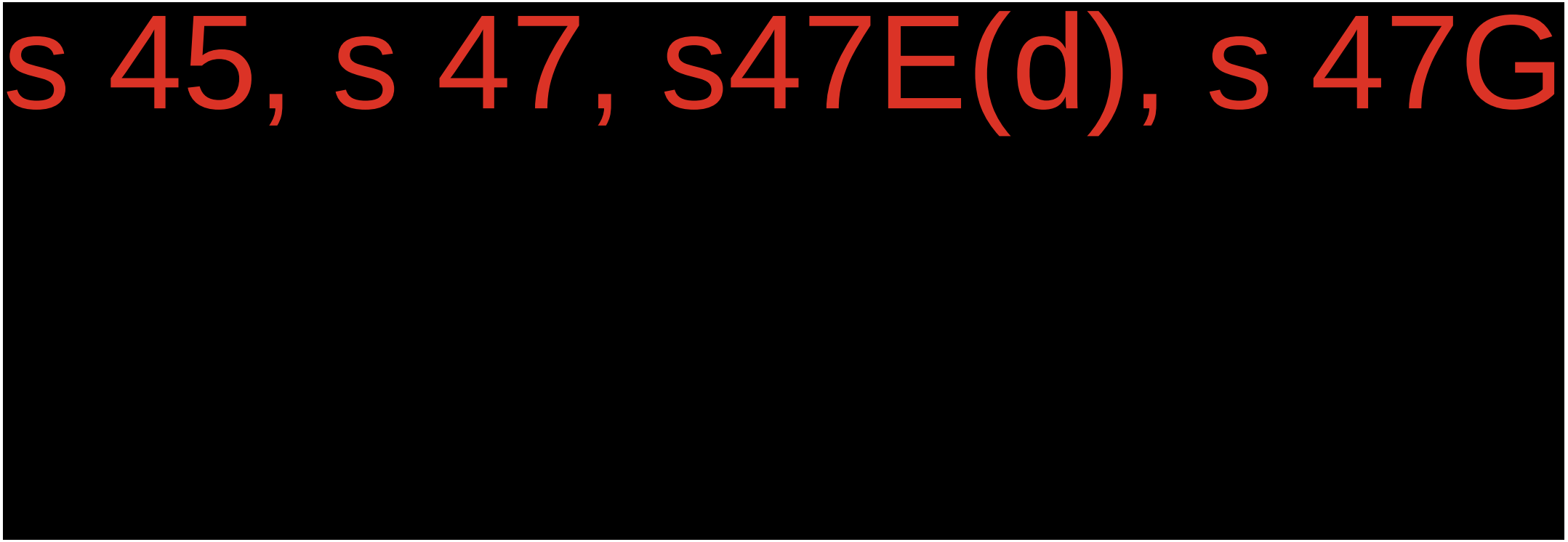
Copyright © 2025 Accenture. All rights reserved.



Copyright © 2025 Accenture. All rights reserved.



Copyright © 2025 Accenture. All rights reserved.



Copyright © 2025 Accenture. All rights reserved.