Pronounced as "Re-Sea," then you might be talking about an **RACI** chart. RACI stands for Responsible, Accountable, Consulted, and Informed. It’s a matrix used to delineate the roles and responsibilities of individuals in a project or a process, ensuring that everyone knows what they are expected to do.

The RACI chart serves as a tool to help manage expectations and tasks in project management, much like how a syllabus outlines roles and responsibilities in an educational context. Each letter in RACI represents a level of task responsibility:

* **Responsible**: The person(s) who actually completes the task.
* **Accountable**: The person who is ultimately accountable and has Yes/No/Veto authority on the work.
* **Consulted**: People whose opinions are sought; typically subject matter experts.
* **Informed**: People who are kept up-to-date on progress, often only on completion of the task or deliverable.

In the context of Identity and Access Management (IAM), a RACI chart is used to clearly define roles and responsibilities regarding the management of identities, access rights, security policies, and compliance within an organization. Here's an example of what a RACI chart might look like for a typical IAM project:

### **RACI Chart for Identity and Access Management (IAM) Project**

| **Task** | **IAM Manager** | **Security Team** | **IT Admin** | **Compliance Officer** | **Department Heads** |
| --- | --- | --- | --- | --- | --- |
| Define access control policies | A | R |  | C | C |
| Implement role-based access controls (RBAC) | A | C | R | C | C |
| Regular audit of access permissions | C | A | R | R |  |
| Review and update access rights | C | A | R | C | C |
| Train employees on security policies | C | A | C |  | R |
| Handle access requests from new employees | C | C | A |  | R |
| Monitor and respond to IAM alerts | C | R | A |  |  |
| Ensure compliance with regulations | C | C |  | A | R |

#### **Legend:**

* **R** = Responsible (does the work)
* **A** = Accountable (final decision and oversight)
* **C** = Consulted (input required)
* **I** = Informed (needs to be kept updated)

### **Key Role Descriptions:**

* **IAM Manager**: Oversees the IAM program, ensuring that access rights are properly managed according to policy.
* **Security Team**: Develops and enforces security policies, performs security audits, and monitors system for security breaches.
* **IT Admin**: Implements changes to access controls, manages user accounts, and maintains the IAM system.
* **Compliance Officer**: Ensures all IAM policies and practices meet legal and regulatory requirements.
* **Department Heads**: Responsible for requesting and approving access rights for their team members, and ensuring their team complies with security policies.

This RACI chart ensures that tasks related to identity and access management are clearly assigned, reducing the risk of security lapses due to unclear responsibilities. It’s a critical tool for maintaining the security integrity of an organization’s IT environment.